T08T90"26E0E860

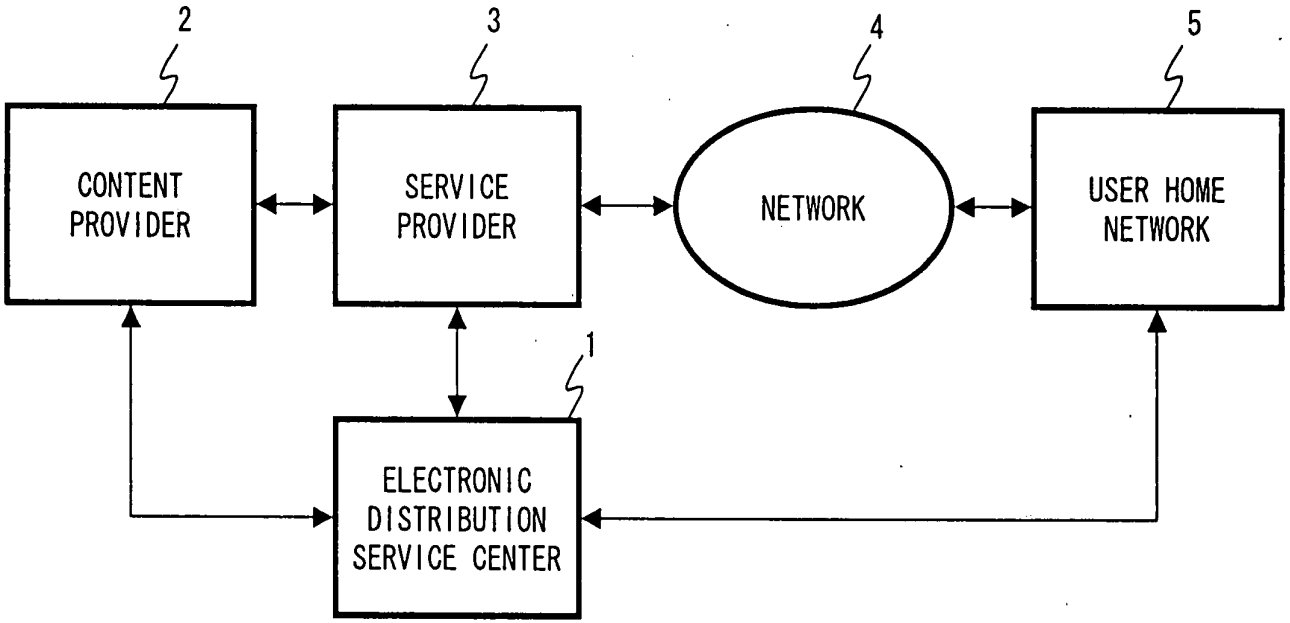

FIG. 1

09/830392

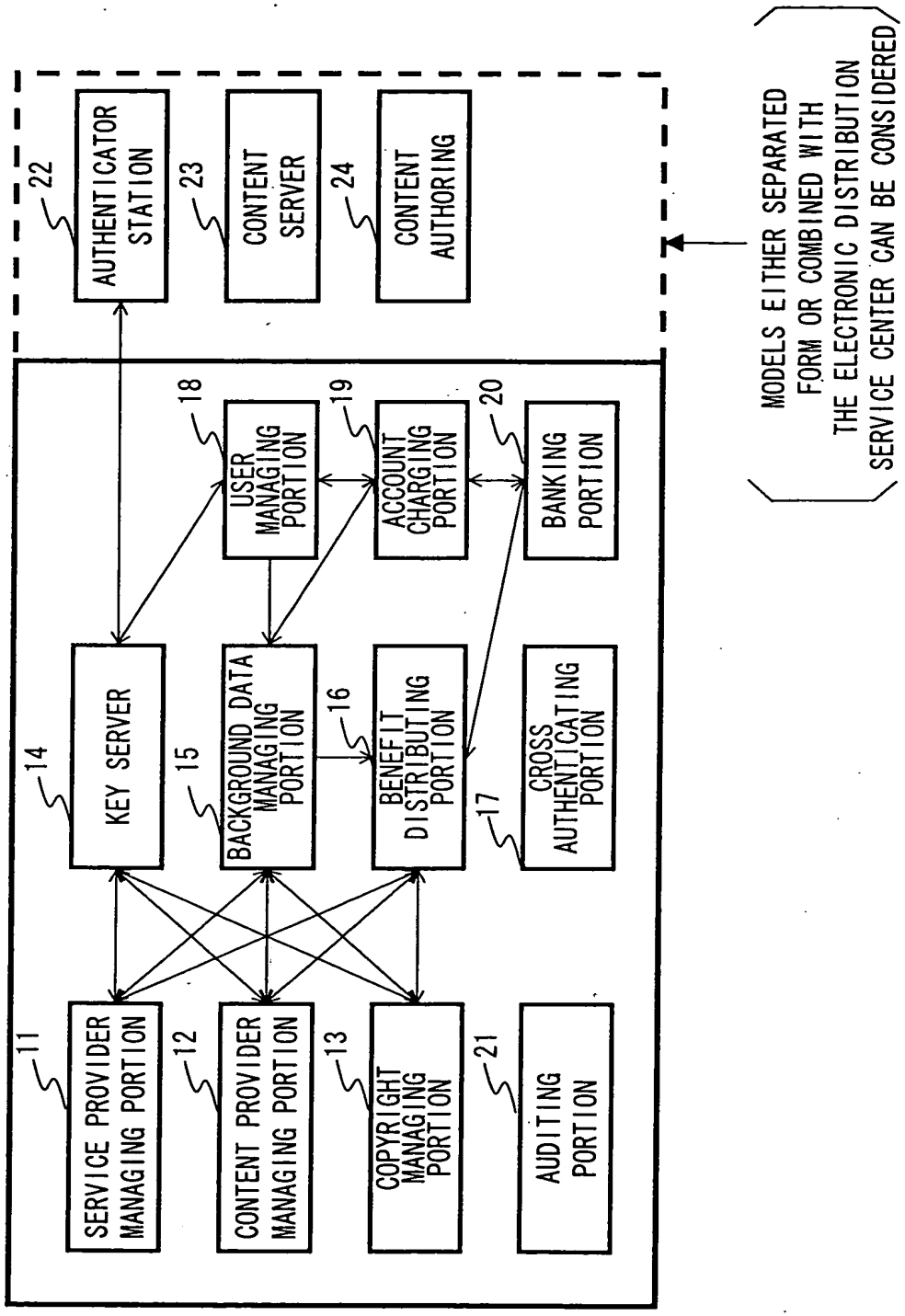
AUTHENTICATOR STATION
22
CONTENT SERVER
23
CONTENT AUTHORING
24
MODELS EITHER SEPARATED FORM OR COMBINED WITH THE ELECTRONIC DISTRIBUTION SERVICE CENTER CAN BE CONSIDERED
USER MANAGING PORTION
18
ACCOUNT CHARGING PORTION
19
BANKING PORTION
20
KEY SERVER
14
BACKGROUND DATA MANAGING PORTION
15
16
BENEFIT DISTRIBUTING PORTION
CROSS AUTHENTICATING PORTION
17
SERVICE PROVIDER MANAGING PORTION
11
CONTENT PROVIDER MANAGING PORTION
12
COPYRIGHT MANAGING PORTION
13
AUDITING PORTION
21

FIG. 2

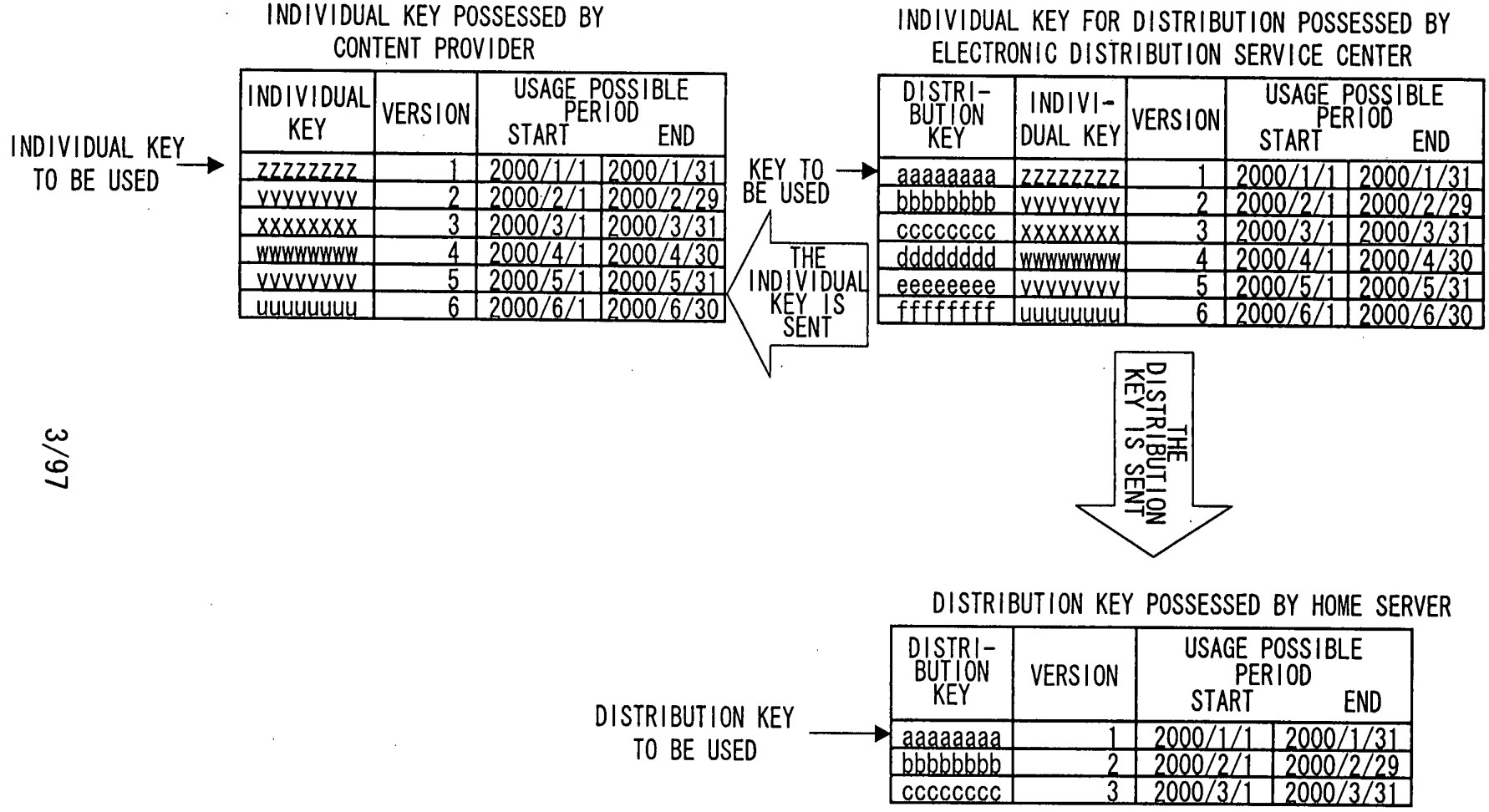
INDIVIDUAL KEY POSSESSED BY CONTENT PROVIDER
INDIVIDUAL KEY TO BE USED
INDIVIDUAL KEY
VERSION
USAGE POSSIBLE PERIOD
START
END
zzzzzzzz 1 2000/1/1 2000/1/31
yyyyyyyy 2 2000/2/1 2000/2/29
xxxxxxxx 3 2000/3/1 2000/3/31
wwwwwwww 4 2000/4/1 2000/4/30
vvvvvvvv 5 2000/5/1 2000/5/31
uuuuuuuu 6 2000/6/1 2000/6/30
KEY TO BE USED
THE INDIVIDUAL KEY IS SENT
INDIVIDUAL KEY FOR DISTRIBUTION POSSESSED BY ELECTRONIC DISTRIBUTION SERVICE CENTER
DISTRI-BUTION KEY
INDIVI-DUAL KEY
VERSION
USAGE POSSIBLE PERIOD
START
END
aaaaaaaa zzzzzzzz 1 2000/1/1 2000/1/31
bbbbbbbb yyyyyyyy 2 2000/2/1 2000/2/29
cccccccc xxxxxxxx 3 2000/3/1 2000/3/31
dddddddd wwwwwwww 4 2000/4/1 2000/4/30
eeeeeeee vvvvvvvv 5 2000/5/1 2000/5/31
ffffffff uuuuuuuu 6 2000/6/1 2000/6/30
THE DISTRIBUTION KEY IS SENT
DISTRIBUTION KEY POSSESSED BY HOME SERVER
DISTRIBUTION KEY TO BE USED
DISTRI-BUTION KEY
VERSION
USAGE POSSIBLE PERIOD
START
END
aaaaaaaa 1 2000/1/1 2000/1/31
bbbbbbbb 2 2000/2/1 2000/2/29
cccccccc 3 2000/3/1 2000/3/31

FIG. 3

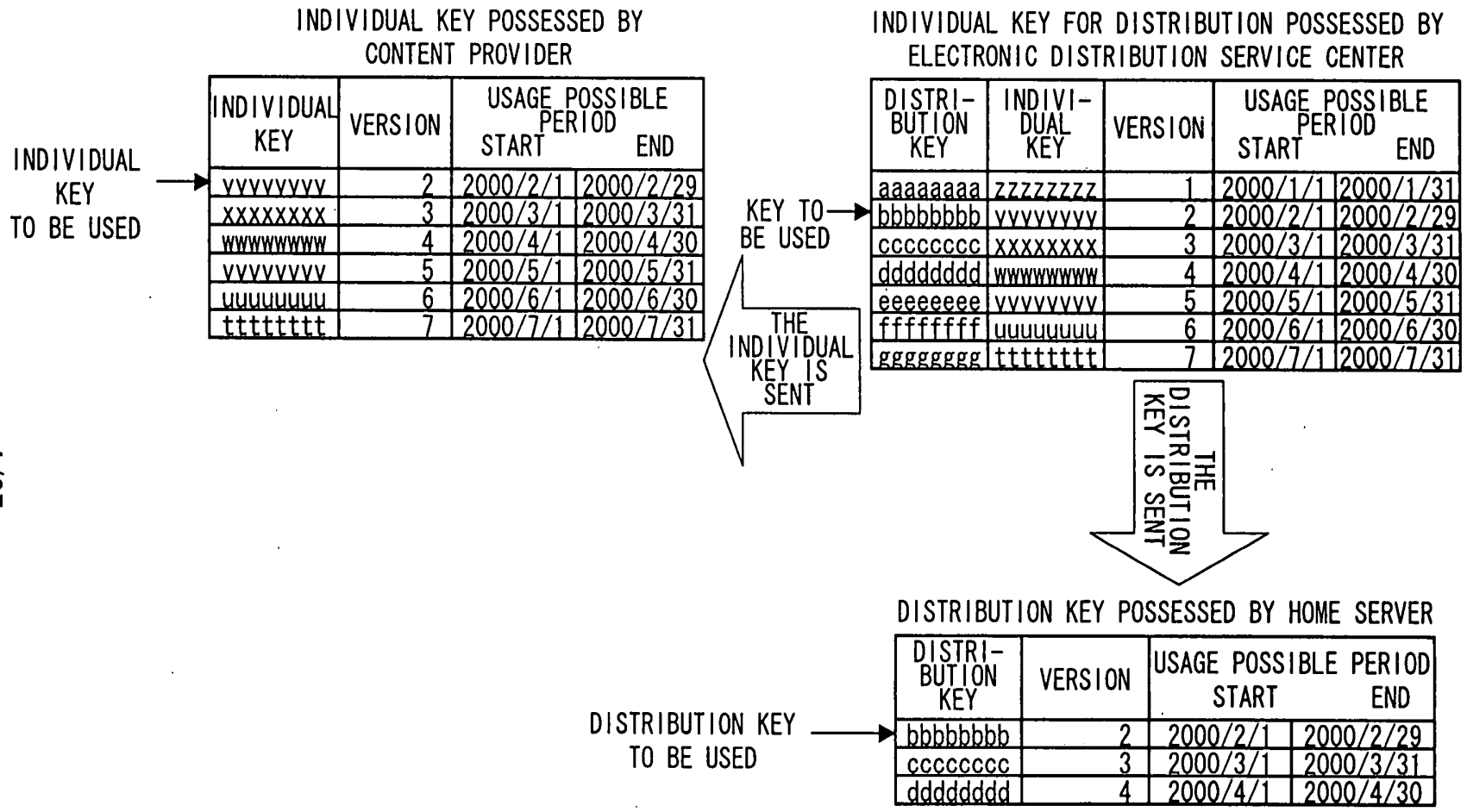
INDIVIDUAL KEY POSSESSED BY CONTENT PROVIDER
INDIVIDUAL KEY TO BE USED
INDIVIDUAL KEY
VERSION
USAGE POSSIBLE PERIOD START
END
vvvvvvvv 2 2000/2/1 2000/2/29
xxxxxxxx 3 2000/3/1 2000/3/31
wwwwwwww 4 2000/4/1 2000/4/30
vvvvvvvv 5 2000/5/1 2000/5/31
uuuuuuuu 6 2000/6/1 2000/6/30
tttttttt 7 2000/7/1 2000/7/31
KEY TO BE USED
THE INDIVIDUAL KEY IS SENT
INDIVIDUAL KEY FOR DISTRIBUTION POSSESSED BY ELECTRONIC DISTRIBUTION SERVICE CENTER
DISTRI-BUTION KEY
INDIVI-DUAL KEY
VERSION
USAGE POSSIBLE PERIOD START
END
aaaaaaaa zzzzzzzz 1 2000/1/1 2000/1/31
bbbbbbbb vvvvvvvv 2 2000/2/1 2000/2/29
cccccccc xxxxxxxx 3 2000/3/1 2000/3/31
dddddddd wwwwwwww 4 2000/4/1 2000/4/30
eeeeeeee vvvvvvvv 5 2000/5/1 2000/5/31
ffffffff uuuuuuuu 6 2000/6/1 2000/6/30
gggggggg tttttttt 7 2000/7/1 2000/7/31
THE DISTRIBUTION KEY IS SENT
DISTRIBUTION KEY POSSESSED BY HOME SERVER
DISTRIBUTION KEY TO BE USED
DISTRI-BUTION KEY
VERSION
USAGE POSSIBLE PERIOD START
END
bbbbbbbb 2 2000/2/1 2000/2/29
cccccccc 3 2000/3/1 2000/3/31
dddddddd 4 2000/4/1 2000/4/30

FIG. 4

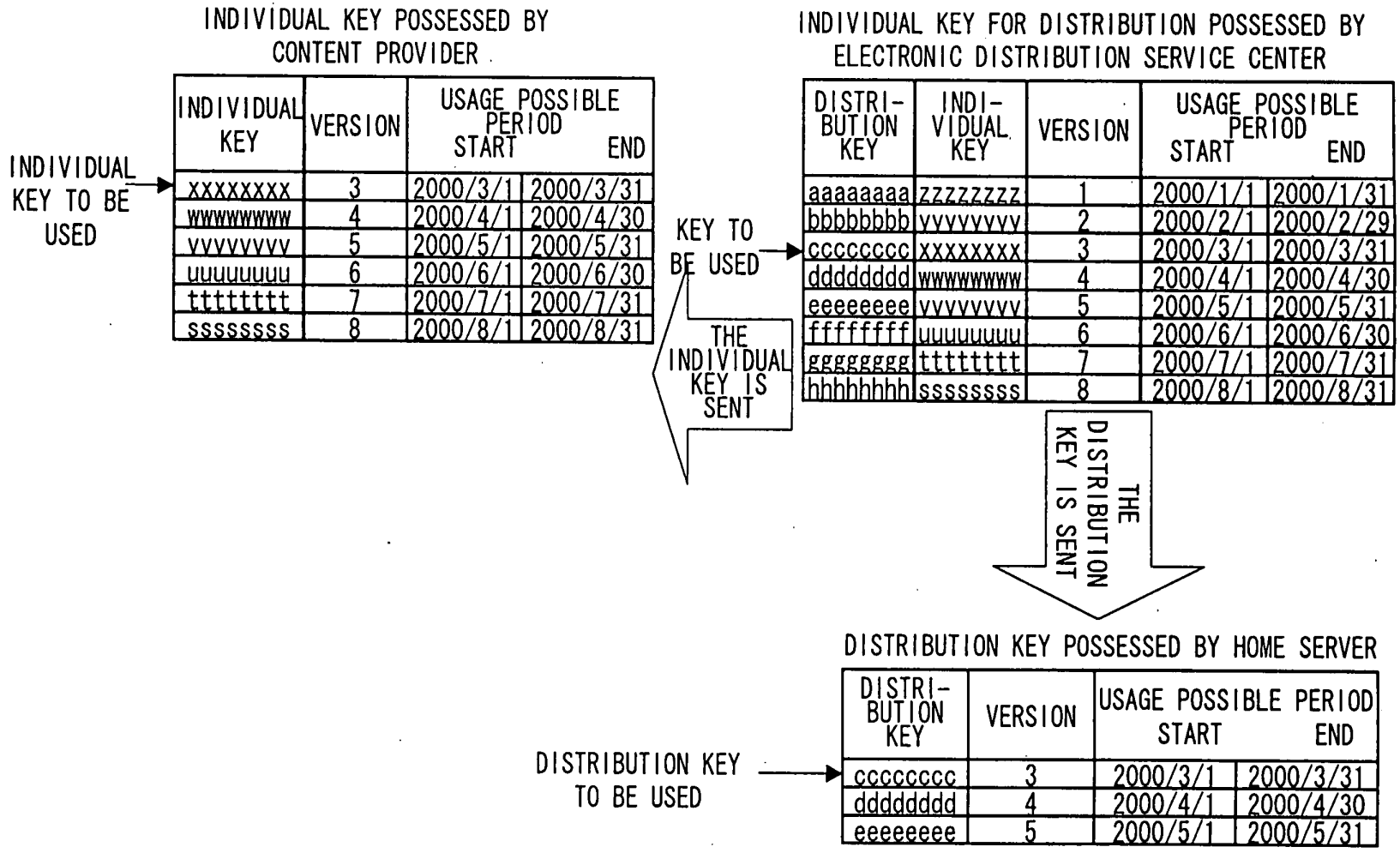
INDIVIDUAL KEY POSSESSED BY CONTENT PROVIDER
INDIVIDUAL KEY TO BE USED
INDIVIDUAL KEY
VERSION
USAGE POSSIBLE PERIOD START
END
xxxxxxxx 3 2000/3/1 2000/3/31
wwwwwwww 4 2000/4/1 2000/4/30
vvvvvvvv 5 2000/5/1 2000/5/31
uuuuuuuu 6 2000/6/1 2000/6/30
tttttttt 7 2000/7/1 2000/7/31
ssssssss 8 2000/8/1 2000/8/31
KEY TO BE USED
THE INDIVIDUAL KEY IS SENT
INDIVIDUAL KEY FOR DISTRIBUTION POSSESSED BY ELECTRONIC DISTRIBUTION SERVICE CENTER
DISTRI-BUTION KEY
INDI-VIDUAL KEY
VERSION
USAGE POSSIBLE PERIOD START
END
aaaaaaaa zzzzzzzz 1 2000/1/1 2000/1/31
bbbbbbbb yyyyyyyy 2 2000/2/1 2000/2/29
cccccccc xxxxxxxx 3 2000/3/1 2000/3/31
dddddddd wwwwwwww 4 2000/4/1 2000/4/30
eeeeeeee vvvvvvvv 5 2000/5/1 2000/5/31
ffffffff uuuuuuuu 6 2000/6/1 2000/6/30
gggggggg tttttttt 7 2000/7/1 2000/7/31
hhhhhhhh ssssssss 8 2000/8/1 2000/8/31
THE DISTRIBUTION KEY IS SENT
DISTRIBUTION KEY POSSESSED BY HOME SERVER
DISTRIBUTION KEY TO BE USED
DISTRI-BUTION KEY
VERSION
USAGE POSSIBLE PERIOD START
END
cccccccc 3 2000/3/1 2000/3/31
dddddddd 4 2000/4/1 2000/4/30
eeeeeeee 5 2000/5/1 2000/5/31

FIG. 5

T08T90" 26E0E860

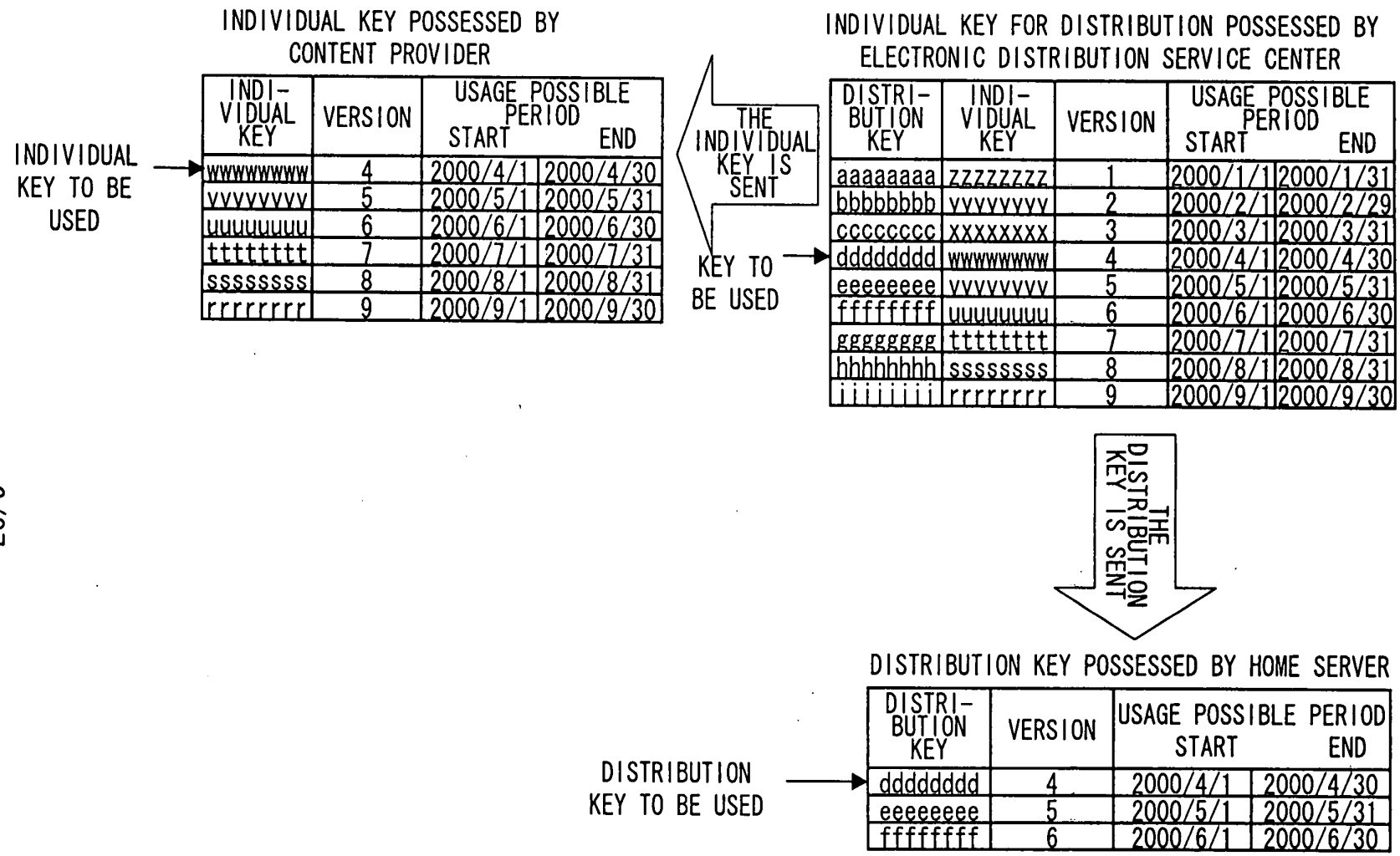

FIG. 6

09/830392

GROUP ID	ID	CONNECTION TO SERVICE CENTER	SETTLEMENT PROCESSING	PURCHASE PROCESSING	PROXY PAYER	PROXY PURCHASER	REGISTRATION
GpID1	ID1	POSSIBLE	POSSIBLE	POSSIBLE	—	—	POSSIBLE
	ID2	POSSIBLE	NOT POSSIBLE	POSSIBLE	ID1	—	POSSIBLE
	ID3	POSSIBLE	NOT POSSIBLE	POSSIBLE	ID1	—	NOT POSSIBLE
	ID4	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID1	POSSIBLE
	ID5	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID2	NOT POSSIBLE
GpID2	ID6	POSSIBLE	POSSIBLE	POSSIBLE	—	—	NOT POSSIBLE
	ID7	POSSIBLE	NOT POSSIBLE	POSSIBLE	ID6	—	NOT POSSIBLE
	ID8	POSSIBLE	NOT POSSIBLE	POSSIBLE	ID6	—	POSSIBLE
	ID9	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID6.7.8	NOT POSSIBLE
	ID10	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID6.7.8	POSSIBLE
GpID3	ID11	POSSIBLE	POSSIBLE	POSSIBLE	—	—	NOT POSSIBLE
	ID12	POSSIBLE	NOT POSSIBLE	POSSIBLE	ID11	—	NOT POSSIBLE
	ID13	POSSIBLE	NOT POSSIBLE	POSSIBLE	ID11	—	POSSIBLE
	ID14	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID11.12.13	NOT POSSIBLE
	ID15	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID11	POSSIBLE
			• • •				

FIG. 7

(A)

GROUP ID	I D	CONNECTION TO SERVICE CENTER	SETTLEMENT PROCESSING	SETTLEMENT ID	PURCHASE PROCESSING	PROXY PAYER	PROXY PURCHASER	REGIS-TRATION	SIG-NATURE
GpID1	ID1	POSSIBLE	POSSIBLE	SETTLEMENT ID 1	POSSIBLE	—	—	POSSIBLE	SIG-NATURE
	ID2	POSSIBLE	NOT POSSIBLE	—	POSSIBLE	ID1	—	POSSIBLE	
	ID3	POSSIBLE	NOT POSSIBLE	—	POSSIBLE	ID1	—	NOT POSSIBLE	
	ID4	NOT POSSIBLE	NOT POSSIBLE	—	NOT POSSIBLE	—	ID1	POSSIBLE	
	ID5	NOT POSSIBLE	NOT POSSIBLE	—	NOT POSSIBLE	—	ID2	NOT POSSIBLE	

(B)

GROUP ID	I D	CONNECTION TO SERVICE CENTER	SETTLEMENT PROCESSING	SETTLEMENT ID	PURCHASE PROCESSING	PROXY PAYER	PROXY PURCHASER	REGIS-TRATION	SIG-NATURE
GpID2	ID6	POSSIBLE	POSSIBLE	SETTLEMENT ID 2	POSSIBLE	—	—	POSSIBLE	SIG-NATURE
	ID7	POSSIBLE	NOT POSSIBLE	—	POSSIBLE	ID6	—	POSSIBLE	
	ID8	POSSIBLE	NOT POSSIBLE	—	POSSIBLE	ID6	—	NOT POSSIBLE	
	ID9	NOT POSSIBLE	NOT POSSIBLE	—	NOT POSSIBLE	—	ID6.7.8	POSSIBLE	
	ID10	NOT POSSIBLE	NOT POSSIBLE	—	NOT POSSIBLE	—	ID6.7.8	NOT POSSIBLE	

FIG. 8

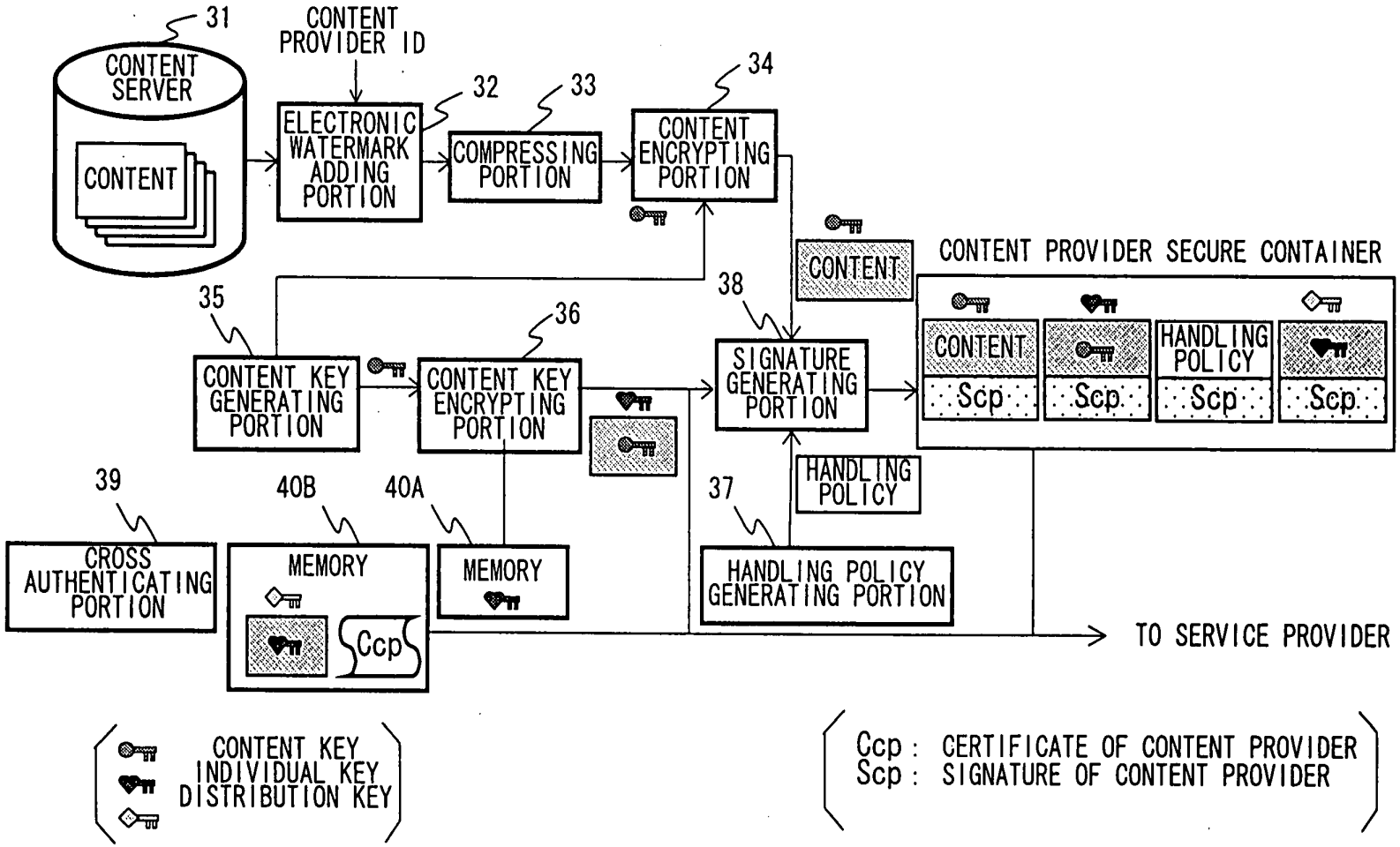
31
CONTENT SERVER
CONTENT
CONTENT PROVIDER ID
ELECTRONIC WATERMARK ADDING PORTION
32
COMPRESSING PORTION
33
CONTENT ENCRYPTING PORTION
34
CONTENT
CONTENT PROVIDER SECURE CONTAINER
35
CONTENT KEY GENERATING PORTION
36
CONTENT KEY ENCRYPTING PORTION
38
SIGNATURE GENERATING PORTION
CONTENT
Scp
Scp
HANDLING POLICY
Scp
Scp
39
CROSS AUTHENTICATING PORTION
40B
MEMORY
Ccp
40A
MEMORY
37
HANDLING POLICY GENERATING PORTION
HANDLING POLICY
TO SERVICE PROVIDER
CONTENT KEY
INDIVIDUAL KEY
DISTRIBUTION KEY
Ccp : CERTIFICATE OF CONTENT PROVIDER
Scp : SIGNATURE OF CONTENT PROVIDER

FIG. 9

(SIGNATURE GENERATION)

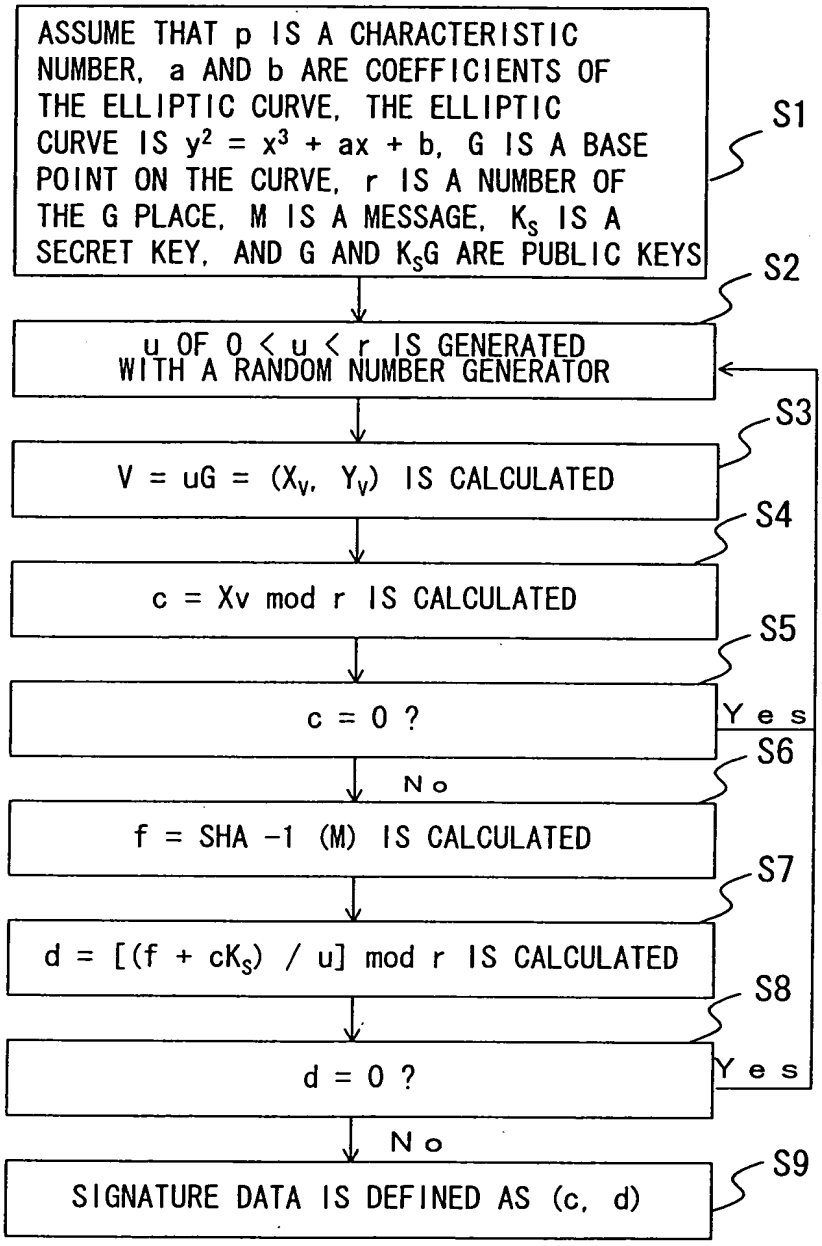

FIG. 10

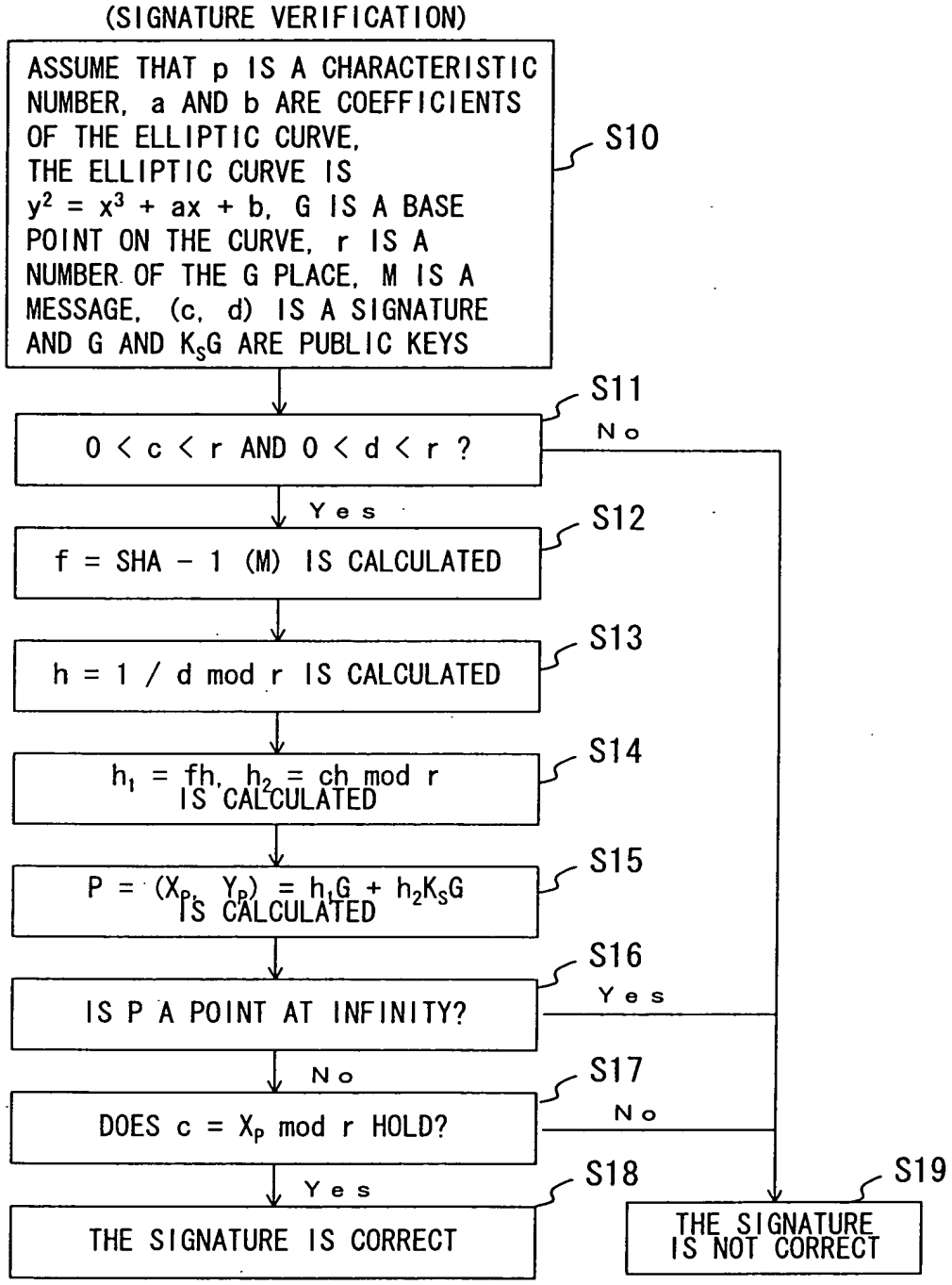
(SIGNATURE VERIFICATION)
ASSUME THAT p IS A CHARACTERISTIC NUMBER, a AND b ARE COEFFICIENTS OF THE ELLIPTIC CURVE, THE ELLIPTIC CURVE IS $y^2 = x^3 + ax + b$, G IS A BASE POINT ON THE CURVE, r IS A NUMBER OF THE G PLACE, M IS A MESSAGE, (c, d) IS A SIGNATURE AND G AND K_SG ARE PUBLIC KEYS
S10
0 < c < r AND 0 < d < r ?
S11
No
Yes
f = SHA - 1 (M) IS CALCULATED
S12
h = 1 / d mod r IS CALCULATED
S13
$h_1 = fh$, $h_2 = ch$ mod r IS CALCULATED
S14
$P = (X_P, Y_P) = h_1G + h_2K_SG$ IS CALCULATED
S15
IS P A POINT AT INFINITY?
S16
Yes
No
DOES $c = X_P$ mod r HOLD?
S17
No
Yes
THE SIGNATURE IS CORRECT
S18
THE SIGNATURE IS NOT CORRECT
S19

FIG. 11

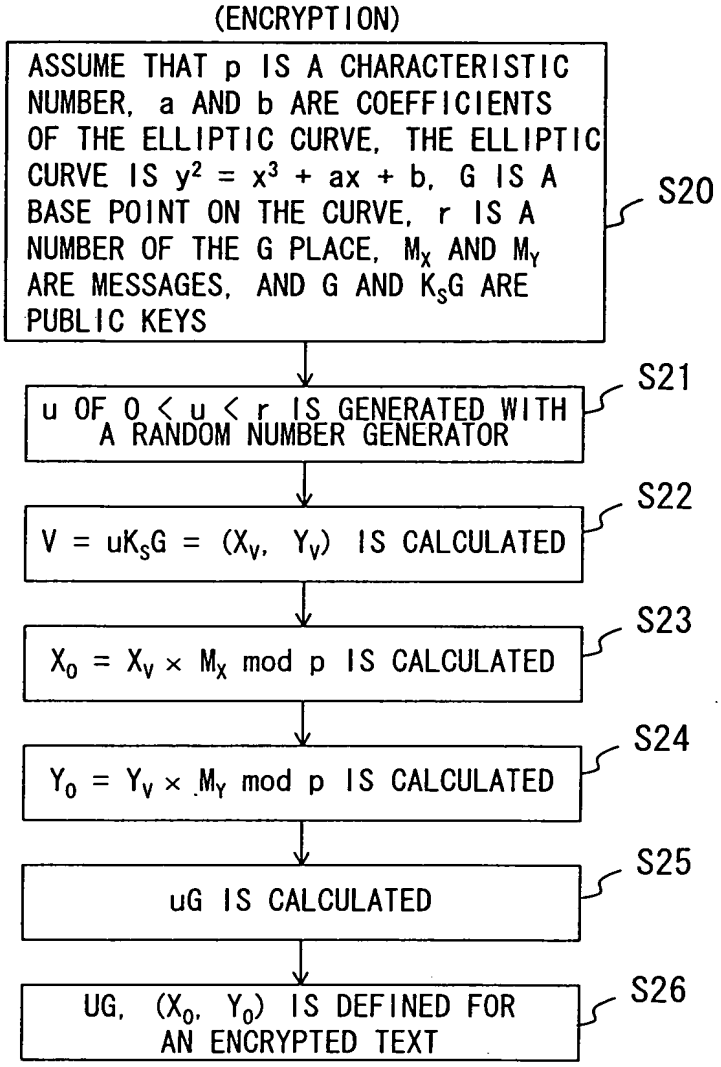
(ENCRYPTION)
ASSUME THAT p IS A CHARACTERISTIC NUMBER, a AND b ARE COEFFICIENTS OF THE ELLIPTIC CURVE, THE ELLIPTIC CURVE IS $y^2 = x^3 + ax + b$, G IS A BASE POINT ON THE CURVE, r IS A NUMBER OF THE G PLACE, M_X AND M_Y ARE MESSAGES, AND G AND K_SG ARE PUBLIC KEYS
S20
u OF $0 < u < r$ IS GENERATED WITH A RANDOM NUMBER GENERATOR
S21
$V = uK_SG = (X_V, Y_V)$ IS CALCULATED
S22
$X_0 = X_V \times M_X \bmod p$ IS CALCULATED
S23
$Y_0 = Y_V \times M_Y \bmod p$ IS CALCULATED
S24
uG IS CALCULATED
S25
UG, (X_0, Y_0) IS DEFINED FOR AN ENCRYPTED TEXT
S26

FIG. 12

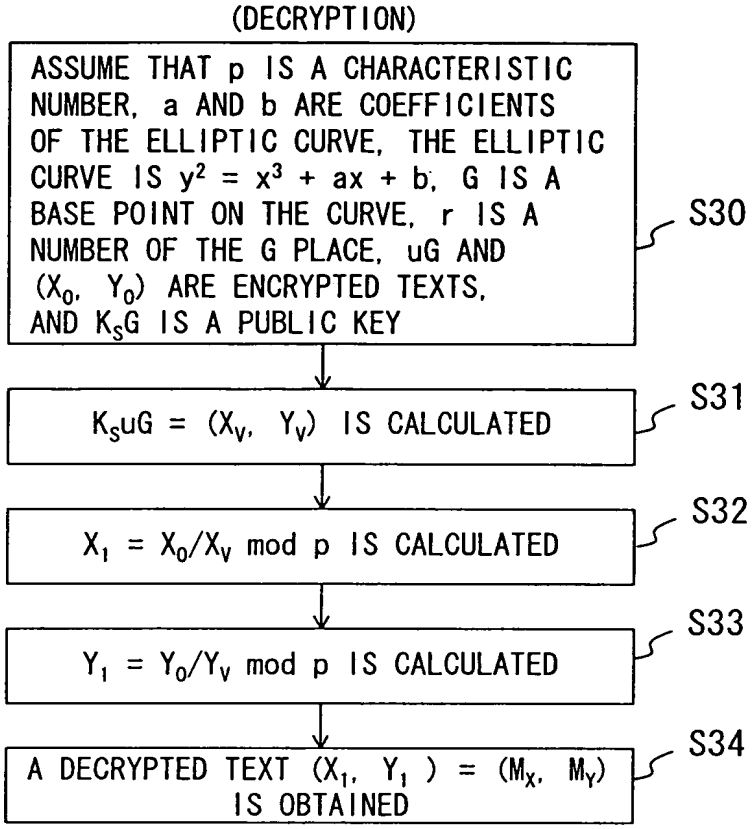
(DECRYPTION)
ASSUME THAT p IS A CHARACTERISTIC NUMBER, a AND b ARE COEFFICIENTS OF THE ELLIPTIC CURVE, THE ELLIPTIC CURVE IS $y^2 = x^3 + ax + b$, G IS A BASE POINT ON THE CURVE, r IS A NUMBER OF THE G PLACE, uG AND (X_0, Y_0) ARE ENCRYPTED TEXTS, AND K_SG IS A PUBLIC KEY
S30
$K_SuG = (X_V, Y_V)$ IS CALCULATED
S31
$X_1 = X_0/X_V \bmod p$ IS CALCULATED
S32
$Y_1 = Y_0/Y_V \bmod p$ IS CALCULATED
S33
A DECRYPTED TEXT $(X_1, Y_1) = (M_X, M_Y)$ IS OBTAINED
S34

FIG. 13

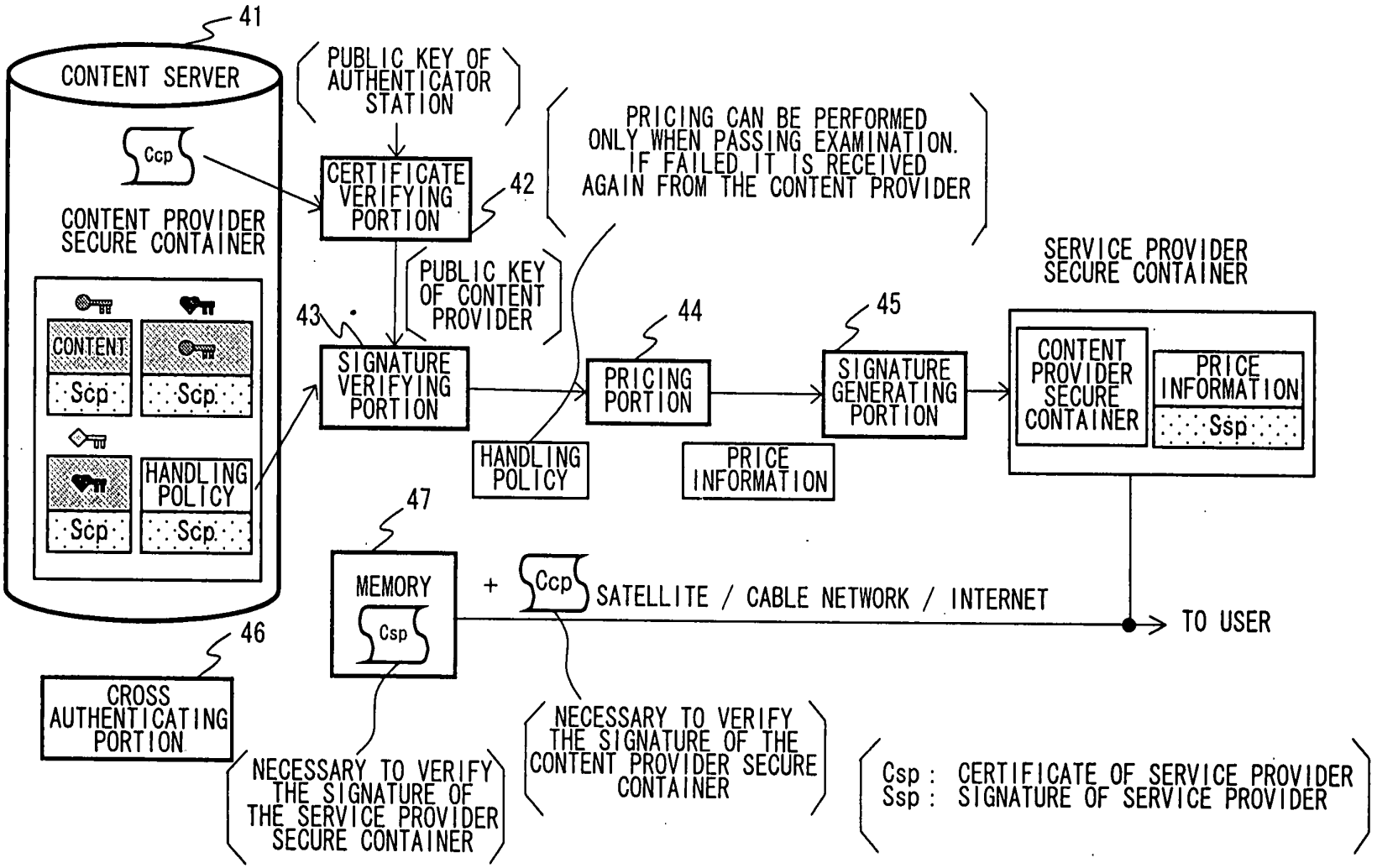
41
CONTENT SERVER
Ccp
CONTENT PROVIDER SECURE CONTAINER
CONTENT
Scp
Scp
Scp
HANDLING POLICY
Scp
PUBLIC KEY OF AUTHENTICATOR STATION
CERTIFICATE VERIFYING PORTION
42
PUBLIC KEY OF CONTENT PROVIDER
43
SIGNATURE VERIFYING PORTION
PRICING CAN BE PERFORMED ONLY WHEN PASSING EXAMINATION. IF FAILED IT IS RECEIVED AGAIN FROM THE CONTENT PROVIDER
HANDLING POLICY
44
PRICING PORTION
PRICE INFORMATION
45
SIGNATURE GENERATING PORTION
SERVICE PROVIDER SECURE CONTAINER
CONTENT PROVIDER SECURE CONTAINER
PRICE INFORMATION
Ssp
47
MEMORY
Csp
+
Ccp
SATELLITE / CABLE NETWORK / INTERNET
TO USER
46
CROSS AUTHENTICATING PORTION
NECESSARY TO VERIFY THE SIGNATURE OF THE SERVICE PROVIDER SECURE CONTAINER
NECESSARY TO VERIFY THE SIGNATURE OF THE CONTENT PROVIDER SECURE CONTAINER
Csp : CERTIFICATE OF SERVICE PROVIDER
Ssp : SIGNATURE OF SERVICE PROVIDER

FIG. 14

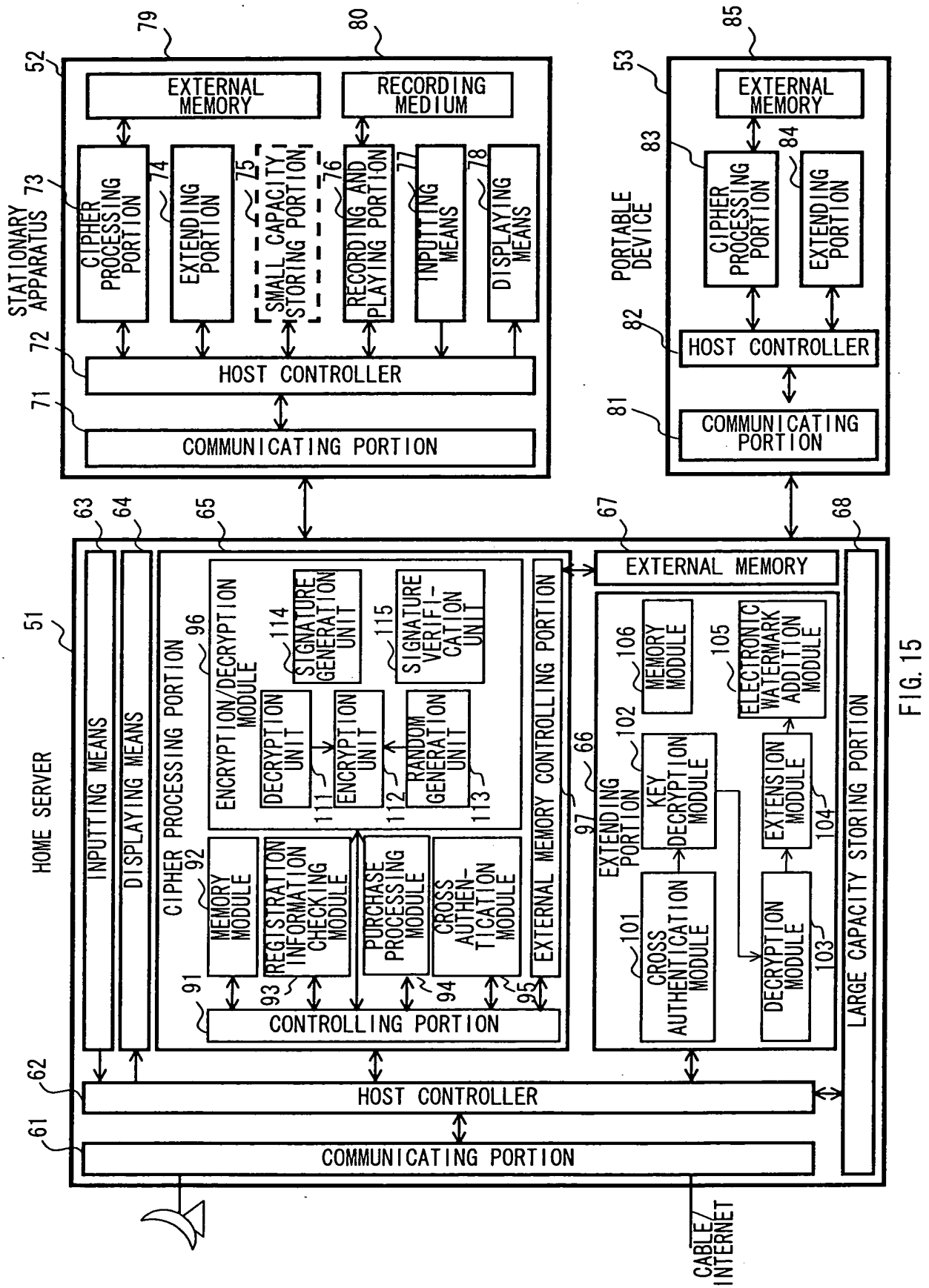
STATIONARY APPARATUS
52
79
80
EXTERNAL MEMORY
RECORDING MEDIUM
CIPHER PROCESSING PORTION
73
74
EXTENDING PORTION
75
SMALL CAPACITY STORING PORTION
76
RECORDING AND PLAYING PORTION
77
INPUTTING MEANS
78
DISPLAYING MEANS
72
HOST CONTROLLER
71
COMMUNICATING PORTION
PORTABLE DEVICE
53
85
EXTERNAL MEMORY
83
84
CIPHER PROCESSING PORTION
EXTENDING PORTION
82
HOST CONTROLLER
81
COMMUNICATING PORTION
HOME SERVER
51
63
64
65
67
68
INPUTTING MEANS
DISPLAYING MEANS
CIPHER PROCESSING PORTION
96
ENCRYPTION/DECRYPTION MODULE
114
SIGNATURE GENERATION UNIT
115
SIGNATURE VERIFICATION UNIT
DECRYPTION UNIT
111
ENCRYPTION UNIT
112
RANDOM GENERATION UNIT
113
EXTERNAL MEMORY CONTROLLING PORTION
EXTERNAL MEMORY
66
97
EXTENDING PORTION
102
KEY DECRYPTION MODULE
106
MEMORY MODULE
105
ELECTRONIC WATERMARK ADDITION MODULE
92
MEMORY MODULE
REGISTRATION INFORMATION CHECKING MODULE
PURCHASE PROCESSING MODULE
CROSS AUTHENTICATION MODULE
101
CROSS AUTHENTICATION MODULE
EXTENSION MODULE
104
DECRYPTION MODULE
103
LARGE CAPACITY STORING PORTION
91
93
94
95
CONTROLLING PORTION
62
HOST CONTROLLER
61
COMMUNICATING PORTION
CABLE/INTERNET

FIG. 15

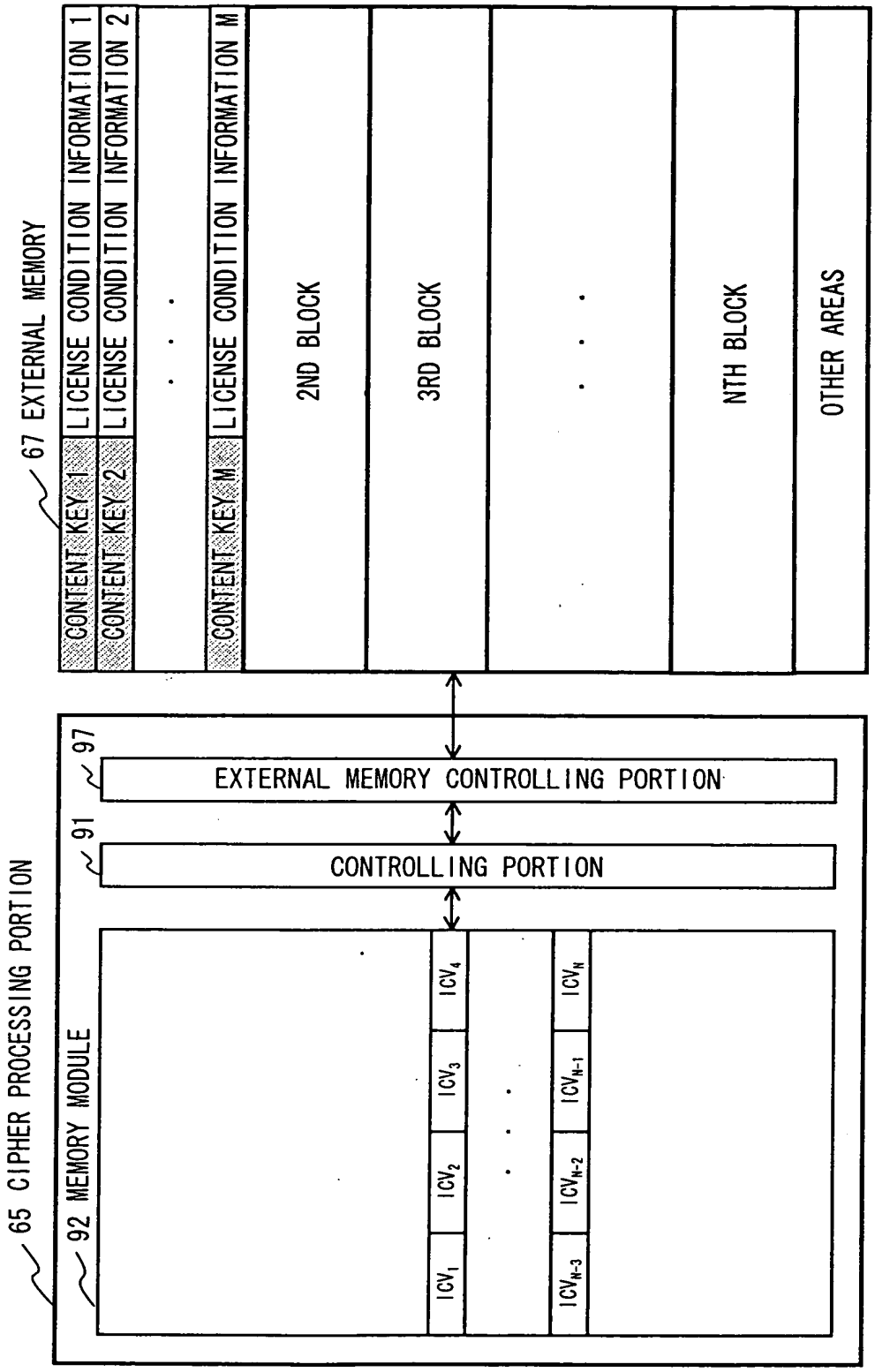
67 EXTERNAL MEMORY
CONTENT KEY 1
LICENSE CONDITION INFORMATION 1
CONTENT KEY 2
LICENSE CONDITION INFORMATION 2
CONTENT KEY M
LICENSE CONDITION INFORMATION M
2ND BLOCK
3RD BLOCK
NTH BLOCK
OTHER AREAS
65 CIPHER PROCESSING PORTION
97
EXTERNAL MEMORY CONTROLLING PORTION
91
CONTROLLING PORTION
92 MEMORY MODULE
ICV1
ICV2
ICV3
ICV4
ICVN-3
ICVN-2
ICVN-1
ICVN

FIG.16

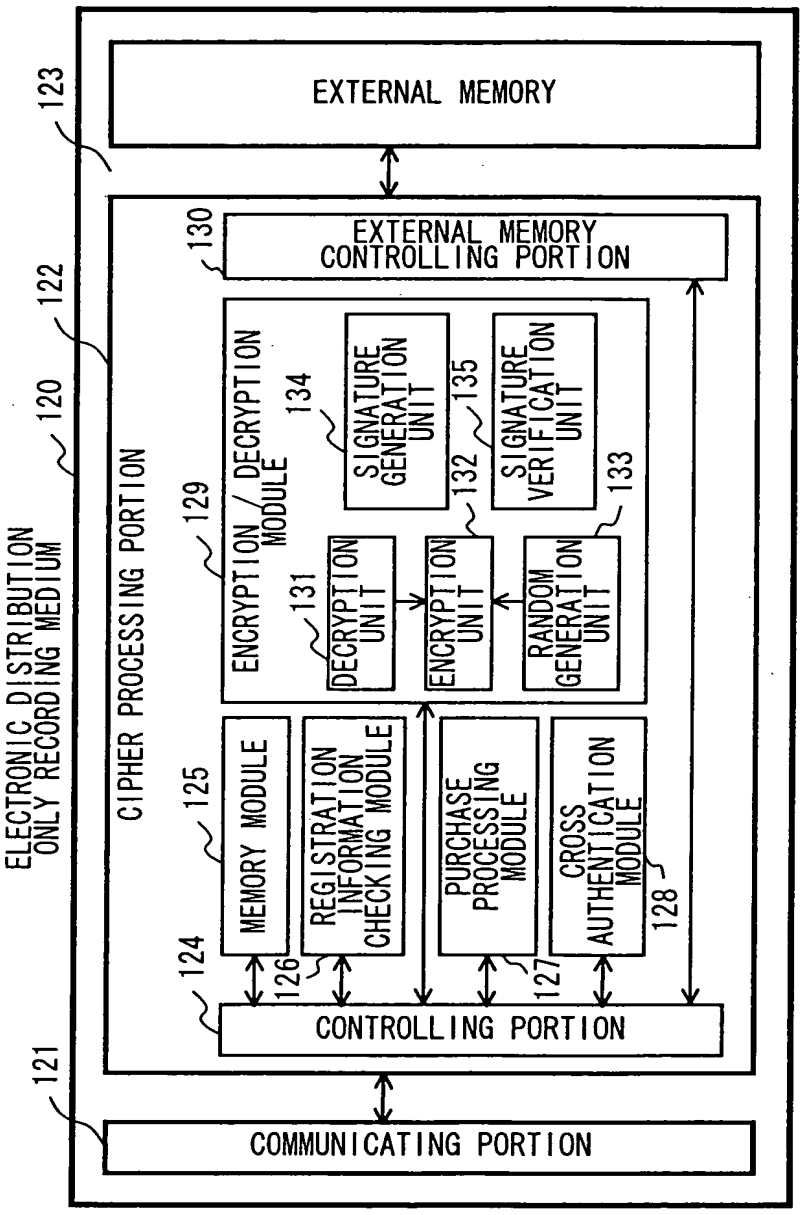
ELECTRONIC DISTRIBUTION ONLY RECORDING MEDIUM
123
EXTERNAL MEMORY
122
120
CIPHER PROCESSING PORTION
130
EXTERNAL MEMORY CONTROLLING PORTION
129
ENCRYPTION / DECRYPTION MODULE
134
SIGNATURE GENERATION UNIT
135
SIGNATURE VERIFICATION UNIT
131
DECRYPTION UNIT
132
ENCRYPTION UNIT
133
RANDOM GENERATION UNIT
125
MEMORY MODULE
126
REGISTRATION INFORMATION CHECKING MODULE
127
PURCHASE PROCESSING MODULE
128
CROSS AUTHENTICATION MODULE
124
CONTROLLING PORTION
121
COMMUNICATING PORTION

FIG. 17

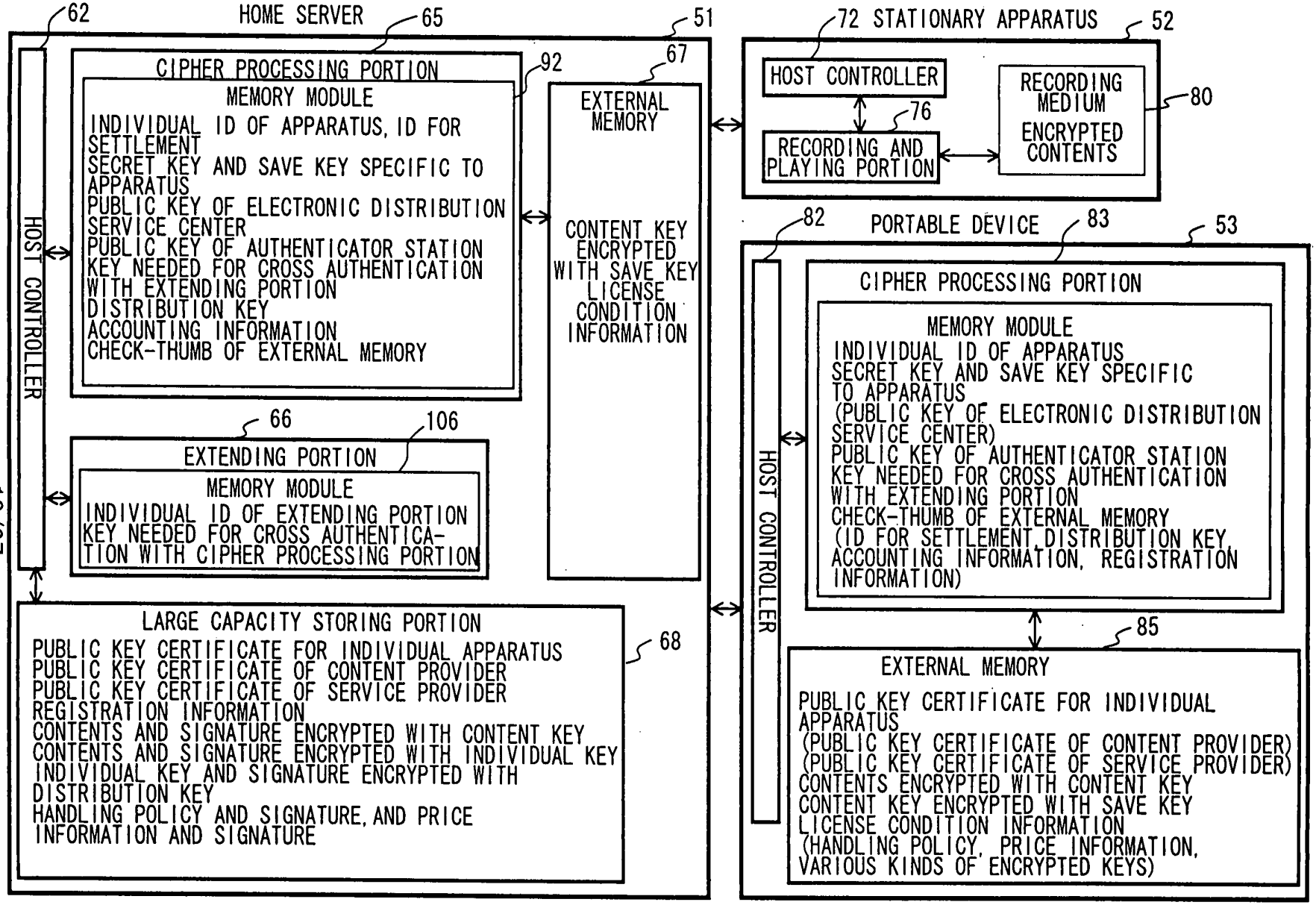
62
HOME SERVER
65
51
72 STATIONARY APPARATUS
52
HOST CONTROLLER
CIPHER PROCESSING PORTION
92
67
EXTERNAL MEMORY
HOST CONTROLLER
76
RECORDING MEDIUM
ENCRYPTED CONTENTS
80
RECORDING AND PLAYING PORTION
MEMORY MODULE
INDIVIDUAL ID OF APPARATUS, ID FOR SETTLEMENT
SECRET KEY AND SAVE KEY SPECIFIC TO APPARATUS
PUBLIC KEY OF ELECTRONIC DISTRIBUTION SERVICE CENTER
PUBLIC KEY OF AUTHENTICATOR STATION
KEY NEEDED FOR CROSS AUTHENTICATION WITH EXTENDING PORTION
DISTRIBUTION KEY
ACCOUNTING INFORMATION
CHECK-THUMB OF EXTERNAL MEMORY
CONTENT KEY ENCRYPTED WITH SAVE KEY
LICENSE CONDITION INFORMATION
82
PORTABLE DEVICE
83
53
CIPHER PROCESSING PORTION
66
106
EXTENDING PORTION
MEMORY MODULE
INDIVIDUAL ID OF EXTENDING PORTION
KEY NEEDED FOR CROSS AUTHENTICATION WITH CIPHER PROCESSING PORTION
MEMORY MODULE
INDIVIDUAL ID OF APPARATUS
SECRET KEY AND SAVE KEY SPECIFIC TO APPARATUS
(PUBLIC KEY OF ELECTRONIC DISTRIBUTION SERVICE CENTER)
PUBLIC KEY OF AUTHENTICATOR STATION
KEY NEEDED FOR CROSS AUTHENTICATION WITH EXTENDING PORTION
CHECK-THUMB OF EXTERNAL MEMORY
(ID FOR SETTLEMENT, DISTRIBUTION KEY, ACCOUNTING INFORMATION, REGISTRATION INFORMATION)
HOST CONTROLLER
85
EXTERNAL MEMORY
PUBLIC KEY CERTIFICATE FOR INDIVIDUAL APPARATUS
(PUBLIC KEY CERTIFICATE OF CONTENT PROVIDER)
(PUBLIC KEY CERTIFICATE OF SERVICE PROVIDER)
CONTENTS ENCRYPTED WITH CONTENT KEY
CONTENT KEY ENCRYPTED WITH SAVE KEY
LICENSE CONDITION INFORMATION
(HANDLING POLICY, PRICE INFORMATION, VARIOUS KINDS OF ENCRYPTED KEYS)
LARGE CAPACITY STORING PORTION
68
PUBLIC KEY CERTIFICATE FOR INDIVIDUAL APPARATUS
PUBLIC KEY CERTIFICATE OF CONTENT PROVIDER
PUBLIC KEY CERTIFICATE OF SERVICE PROVIDER
REGISTRATION INFORMATION
CONTENTS AND SIGNATURE ENCRYPTED WITH CONTENT KEY
CONTENTS AND SIGNATURE ENCRYPTED WITH INDIVIDUAL KEY
INDIVIDUAL KEY AND SIGNATURE ENCRYPTED WITH DISTRIBUTION KEY
HANDLING POLICY AND SIGNATURE, AND PRICE INFORMATION AND SIGNATURE

FIG. 18

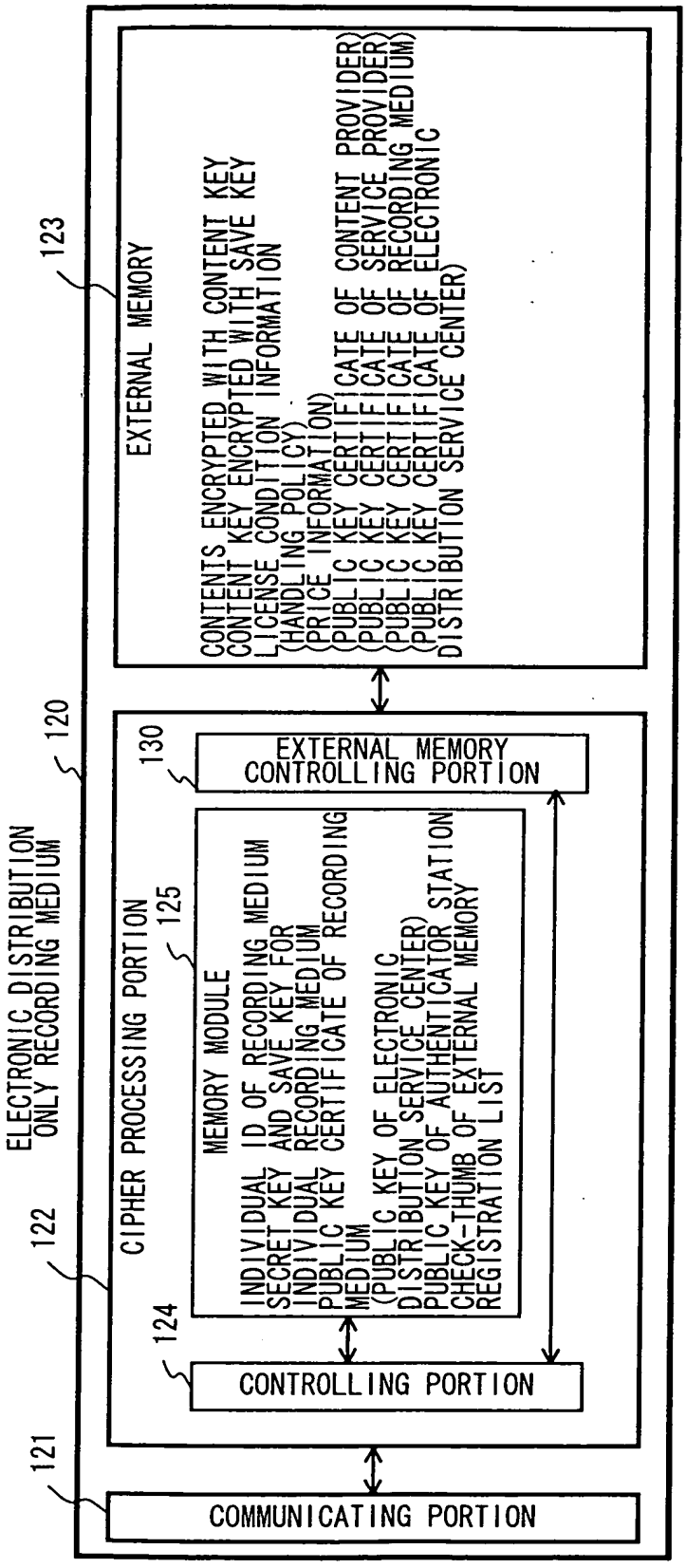
ELECTRONIC DISTRIBUTION ONLY RECORDING MEDIUM
120
121
122
123
124
125
130
EXTERNAL MEMORY
CONTENTS ENCRYPTED WITH CONTENT KEY
CONTENT KEY ENCRYPTED WITH SAVE KEY
LICENSE CONDITION INFORMATION
(HANDLING POLICY)
(PRICE INFORMATION)
(PUBLIC KEY CERTIFICATE OF CONTENT PROVIDER)
(PUBLIC KEY CERTIFICATE OF SERVICE PROVIDER)
(PUBLIC KEY CERTIFICATE OF RECORDING MEDIUM)
(PUBLIC KEY CERTIFICATE OF ELECTRONIC DISTRIBUTION SERVICE CENTER)
EXTERNAL MEMORY CONTROLLING PORTION
CIPHER PROCESSING PORTION
MEMORY MODULE
INDIVIDUAL ID OF RECORDING MEDIUM
SECRET KEY AND SAVE KEY FOR INDIVIDUAL RECORDING MEDIUM
PUBLIC KEY CERTIFICATE OF RECORDING MEDIUM
(PUBLIC KEY OF ELECTRONIC DISTRIBUTION SERVICE CENTER)
PUBLIC KEY OF AUTHENTICATOR STATION
CHECK-THUMB OF EXTERNAL MEMORY REGISTRATION LIST
CONTROLLING PORTION
COMMUNICATING PORTION

FIG. 19

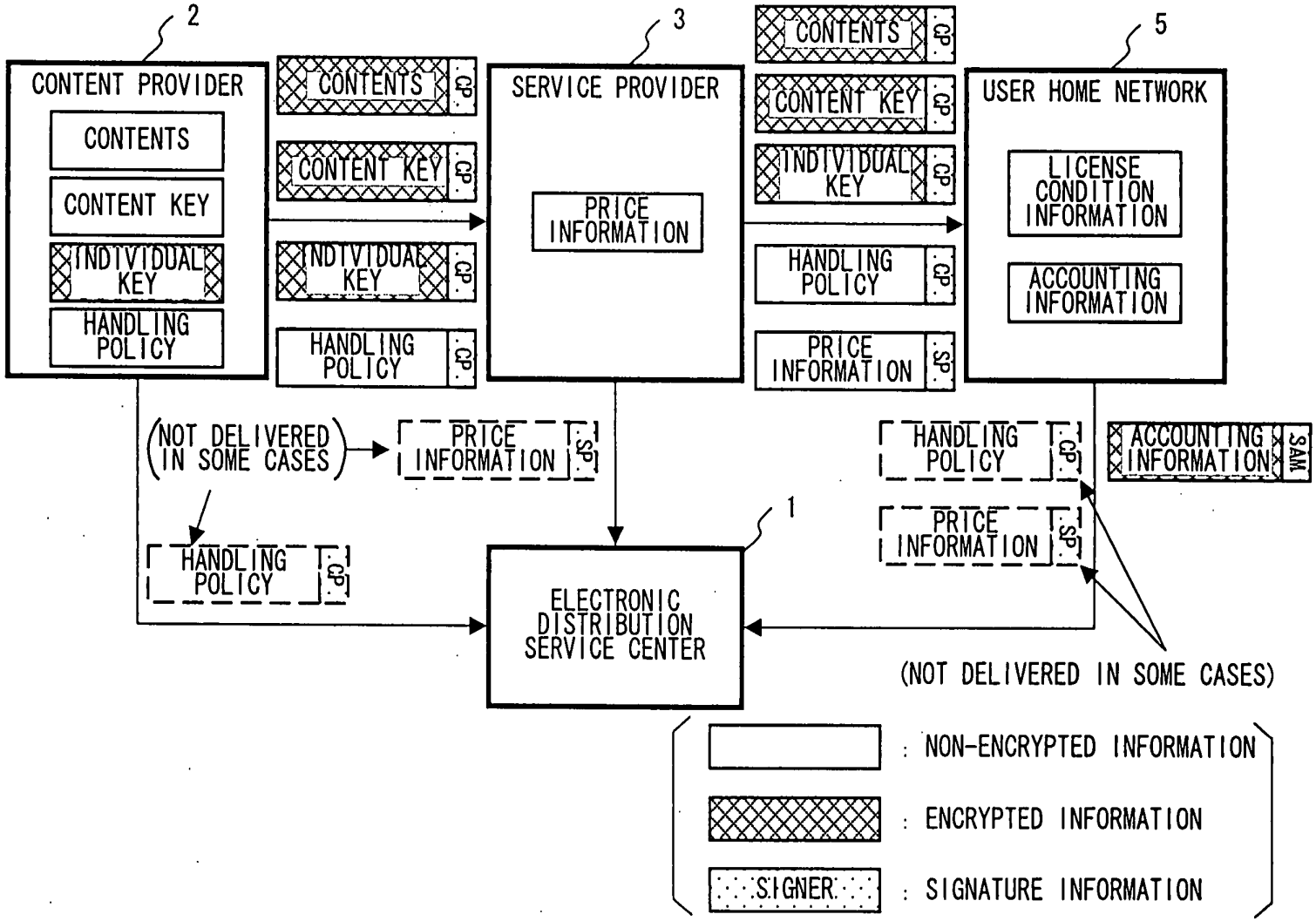
2
CONTENT PROVIDER
CONTENTS
CONTENT KEY
INDIVIDUAL KEY
HANDLING POLICY
CONTENTS CP
CONTENT KEY CP
INDIVIDUAL KEY CP
HANDLING POLICY CP
3
SERVICE PROVIDER
PRICE INFORMATION
CONTENTS CP
CONTENT KEY CP
INDIVIDUAL KEY CP
HANDLING POLICY CP
PRICE INFORMATION SP
5
USER HOME NETWORK
LICENSE CONDITION INFORMATION
ACCOUNTING INFORMATION
(NOT DELIVERED IN SOME CASES)
PRICE INFORMATION SP
HANDLING POLICY CP
HANDLING POLICY CP
ACCOUNTING INFORMATION SAM
PRICE INFORMATION SP
1
ELECTRONIC DISTRIBUTION SERVICE CENTER
(NOT DELIVERED IN SOME CASES)
: NON-ENCRYPTED INFORMATION
: ENCRYPTED INFORMATION
SIGNER
: SIGNATURE INFORMATION

FIG. 20

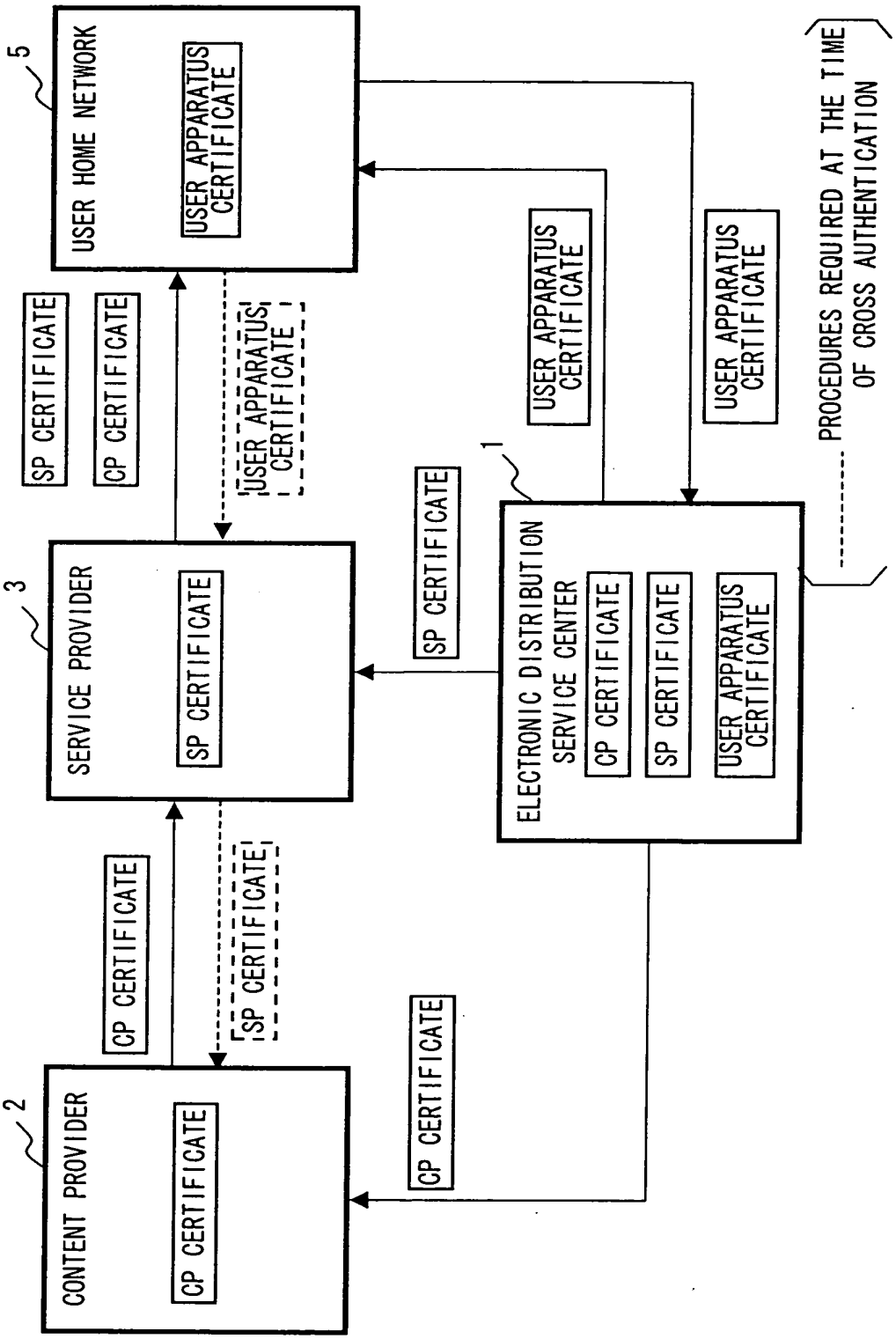
5
USER HOME NETWORK
USER APPARATUS CERTIFICATE
SP CERTIFICATE
CP CERTIFICATE
USER APPARATUS CERTIFICATE
USER APPARATUS CERTIFICATE
USER APPARATUS CERTIFICATE
PROCEDURES REQUIRED AT THE TIME OF CROSS AUTHENTICATION
1
ELECTRONIC DISTRIBUTION SERVICE CENTER
CP CERTIFICATE
SP CERTIFICATE
USER APPARATUS CERTIFICATE
SP CERTIFICATE
3
SERVICE PROVIDER
SP CERTIFICATE
CP CERTIFICATE
SP CERTIFICATE
2
CONTENT PROVIDER
CP CERTIFICATE
CP CERTIFICATE

FIG. 21

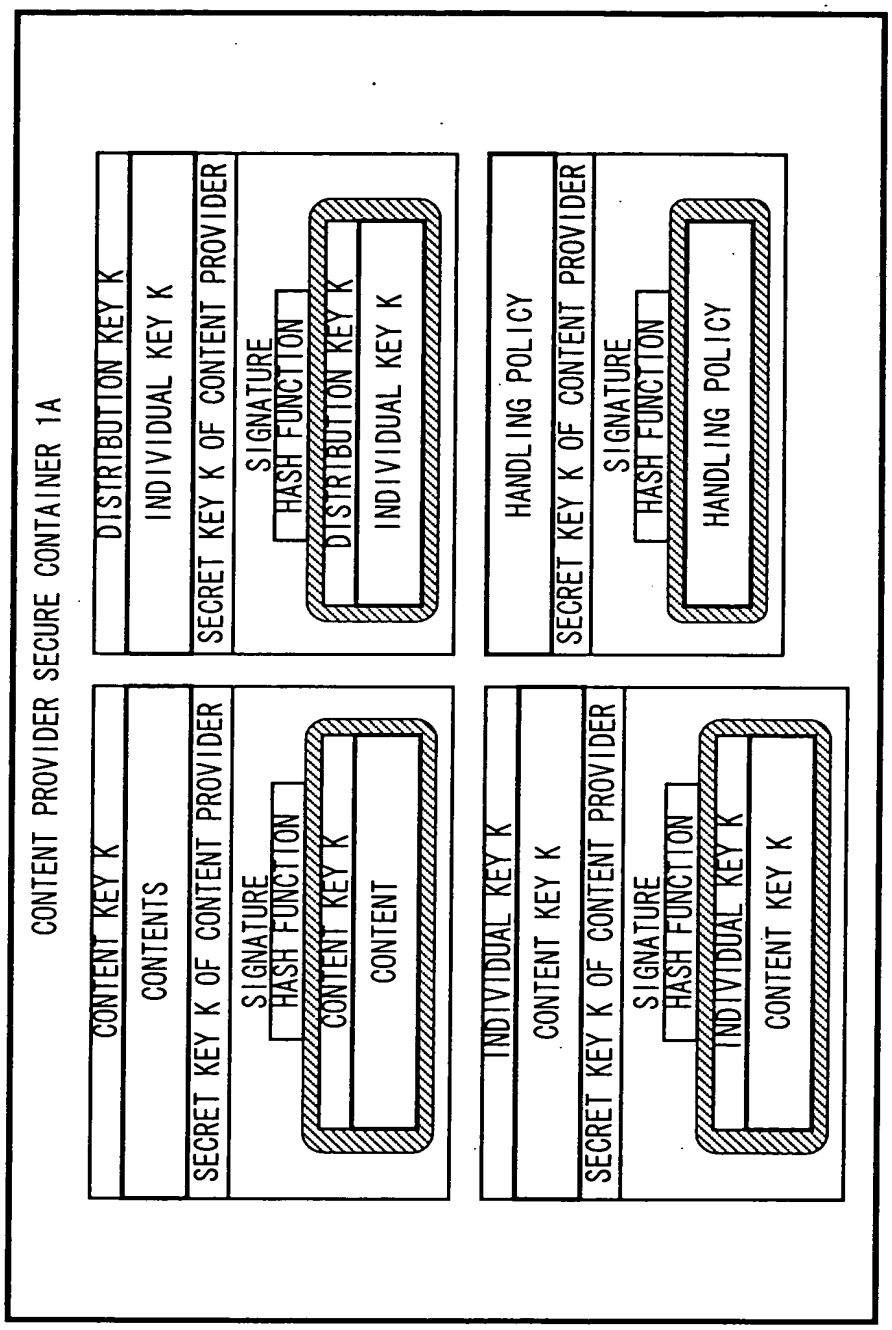
CONTENT PROVIDER SECURE CONTAINER 1A
CONTENT KEY K
CONTENTS
SECRET KEY K OF CONTENT PROVIDER
SIGNATURE
HASH FUNCTION
CONTENT KEY K
CONTENT
DISTRIBUTION KEY K
INDIVIDUAL KEY K
SECRET KEY K OF CONTENT PROVIDER
SIGNATURE
HASH FUNCTION
DISTRIBUTION KEY K
INDIVIDUAL KEY K
INDIVIDUAL KEY K
CONTENT KEY K
SECRET KEY K OF CONTENT PROVIDER
SIGNATURE
HASH FUNCTION
INDIVIDUAL KEY K
CONTENT KEY K
HANDLING POLICY
SECRET KEY K OF CONTENT PROVIDER
SIGNATURE
HASH FUNCTION
HANDLING POLICY

FIG. 22

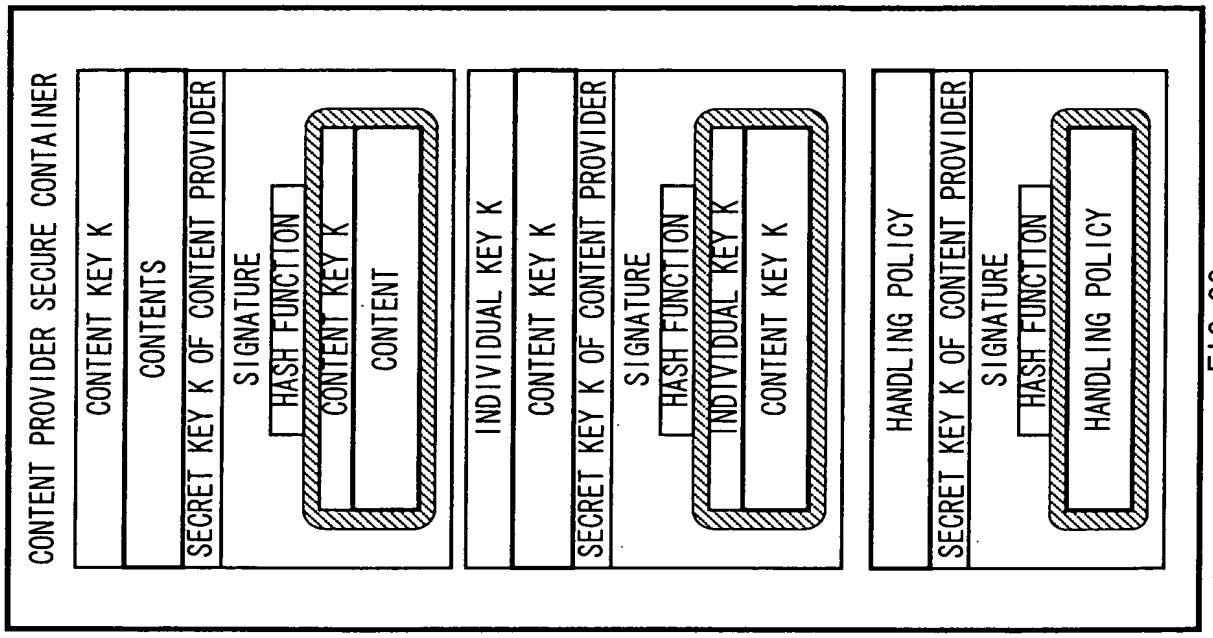

FIG. 23

EP 1 050 794 A2

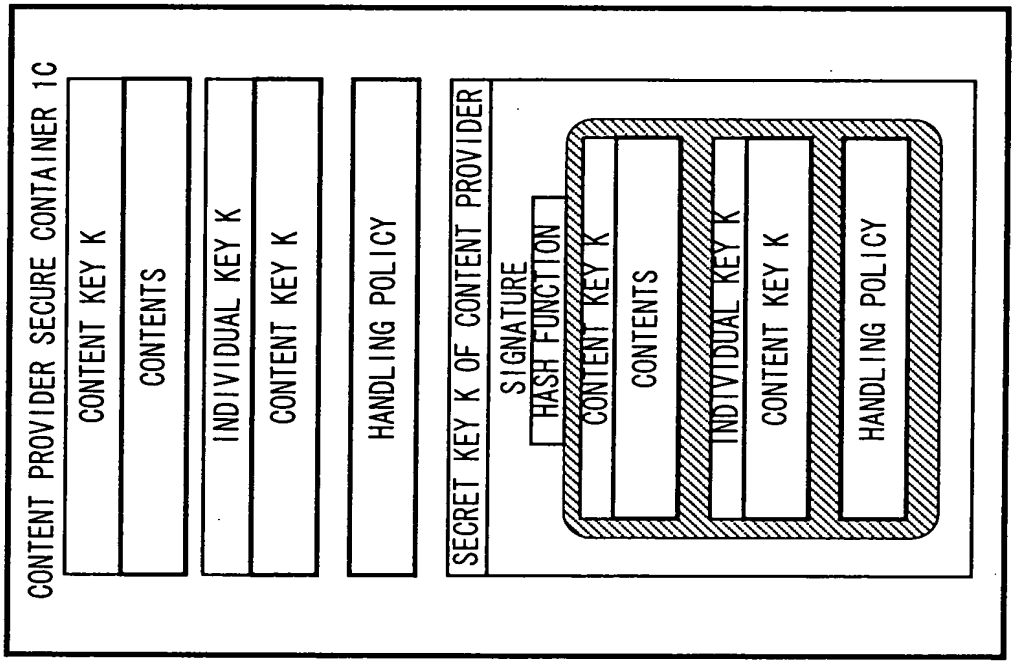
CONTENT PROVIDER SECURE CONTAINER 1C
CONTENT KEY K
CONTENTS
INDIVIDUAL KEY K
CONTENT KEY K
HANDLING POLICY
SECRET KEY K OF CONTENT PROVIDER
SIGNATURE
HASH FUNCTION
CONTENT KEY K
CONTENTS
INDIVIDUAL KEY K
CONTENT KEY K
HANDLING POLICY

FIG. 24

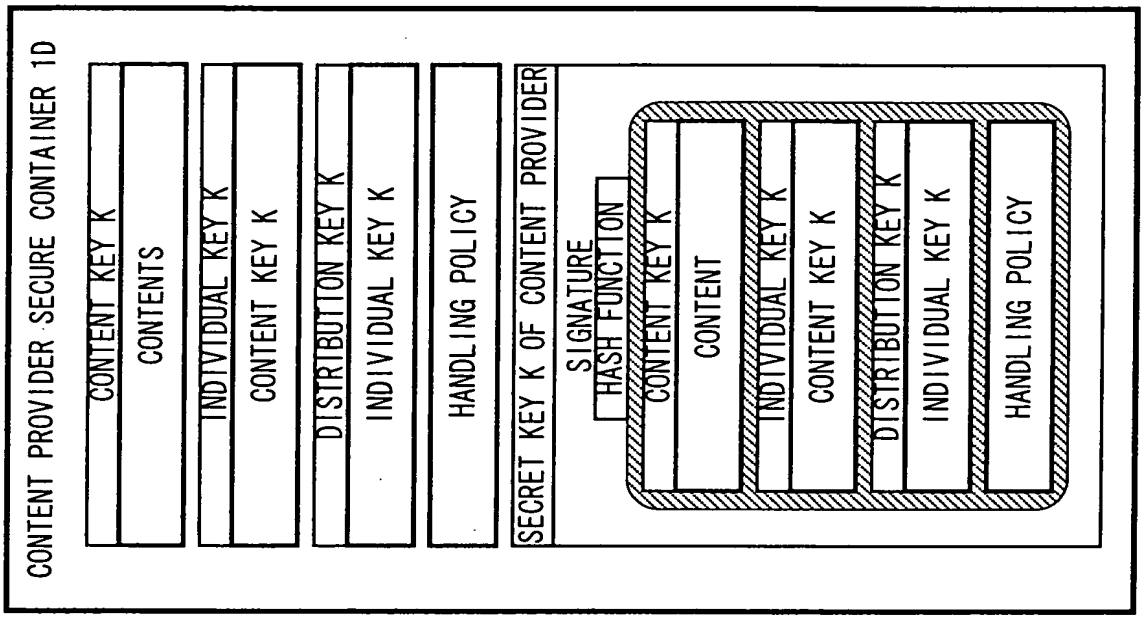
CONTENT PROVIDER SECURE CONTAINER 1D
CONTENT KEY K
CONTENTS
INDIVIDUAL KEY K
CONTENT KEY K
DISTRIBUTION KEY K
INDIVIDUAL KEY K
HANDLING POLICY
SECRET KEY K OF CONTENT PROVIDER
SIGNATURE
HASH FUNCTION
CONTENT KEY K
CONTENT
INDIVIDUAL KEY K
CONTENT KEY K
DISTRIBUTION KEY K
INDIVIDUAL KEY K
HANDLING POLICY

FIG. 25

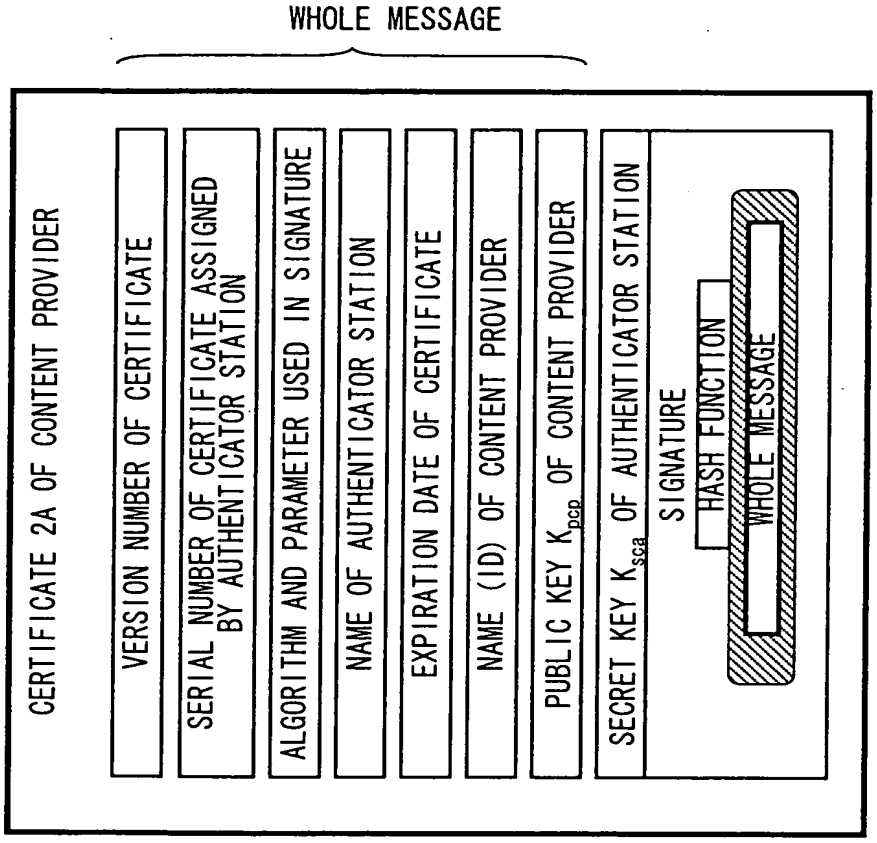
WHOLE MESSAGE
CERTIFICATE 2A OF CONTENT PROVIDER
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ASSIGNED BY AUTHENTICATOR STATION
ALGORITHM AND PARAMETER USED IN SIGNATURE
NAME OF AUTHENTICATOR STATION
EXPIRATION DATE OF CERTIFICATE
NAME (ID) OF CONTENT PROVIDER
PUBLIC KEY K_{pcp} OF CONTENT PROVIDER
SECRET KEY K_{sca} OF AUTHENTICATOR STATION
SIGNATURE
HASH FUNCTION
WHOLE MESSAGE

FIG. 26

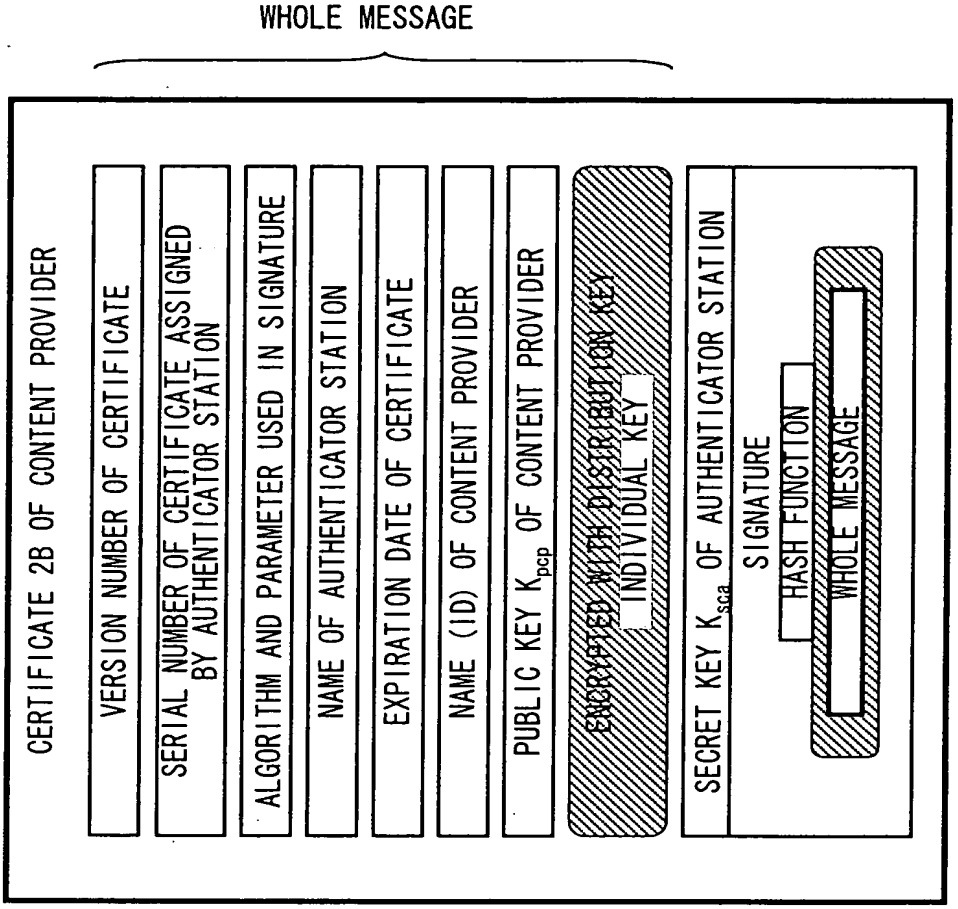
WHOLE MESSAGE
CERTIFICATE 2B OF CONTENT PROVIDER
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ASSIGNED BY AUTHENTICATOR STATION
ALGORITHM AND PARAMETER USED IN SIGNATURE
NAME OF AUTHENTICATOR STATION
EXPIRATION DATE OF CERTIFICATE
NAME (ID) OF CONTENT PROVIDER
PUBLIC KEY K_{pcp} OF CONTENT PROVIDER
ENCRYPTED WITH DISTRIBUTION KEY
INDIVIDUAL KEY
SECRET KEY K_{sca} OF AUTHENTICATOR STATION
SIGNATURE
HASH FUNCTION
WHOLE MESSAGE

FIG. 27

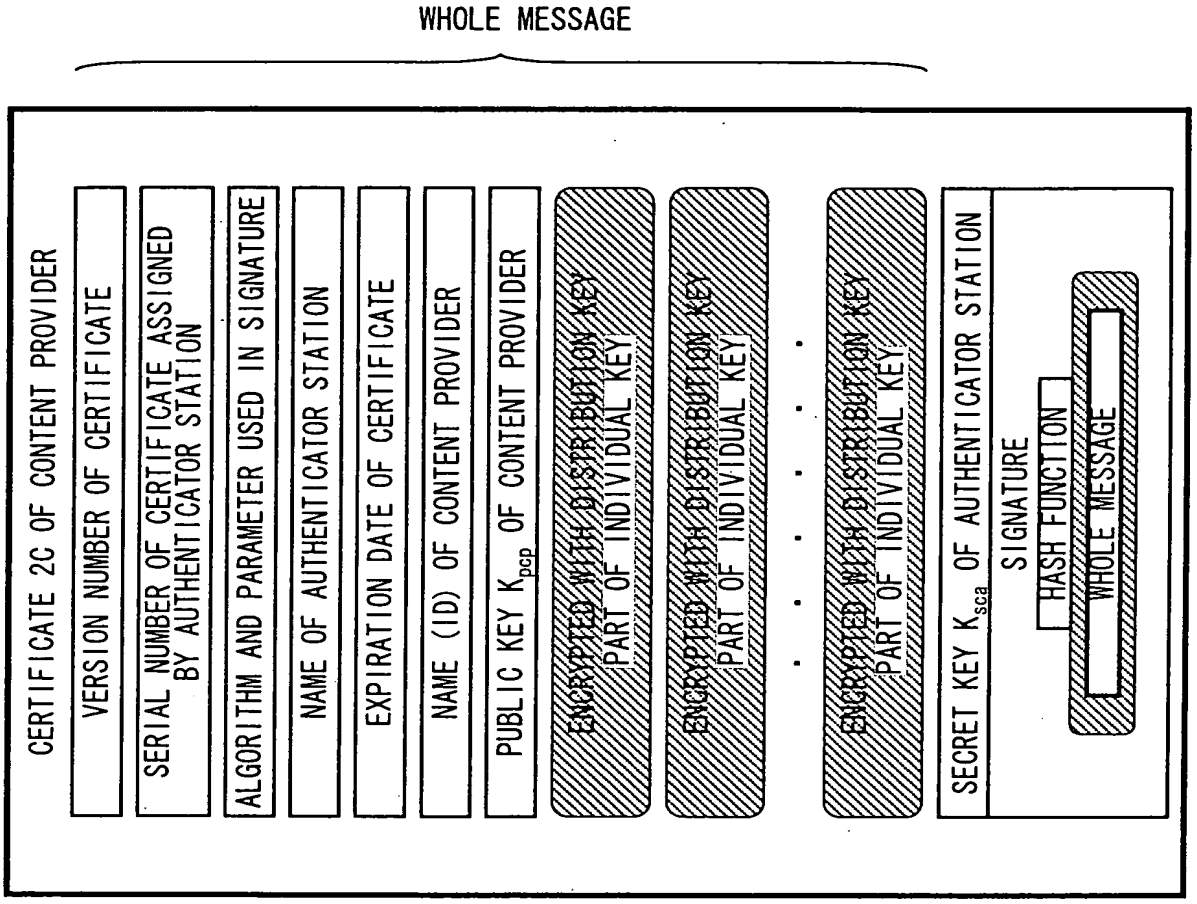

FIG. 28

T0630 "26360

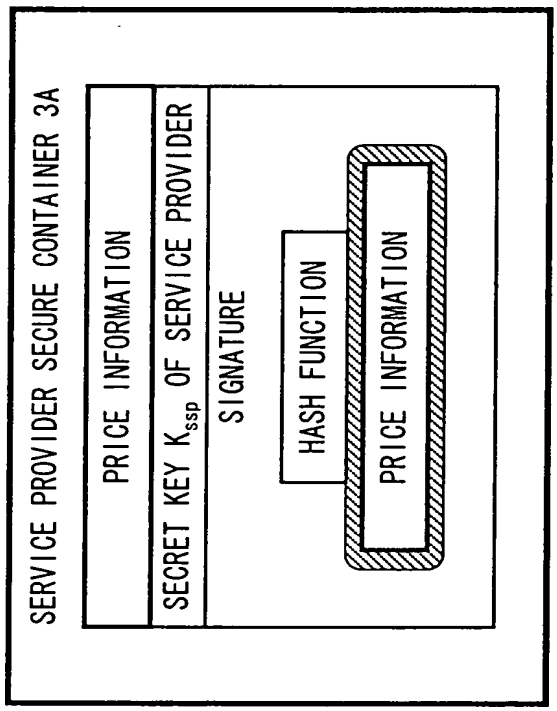
SERVICE PROVIDER SECURE CONTAINER 3A
PRICE INFORMATION
SECRET KEY K_{ssp} OF SERVICE PROVIDER
SIGNATURE
HASH FUNCTION
PRICE INFORMATION

FIG. 29

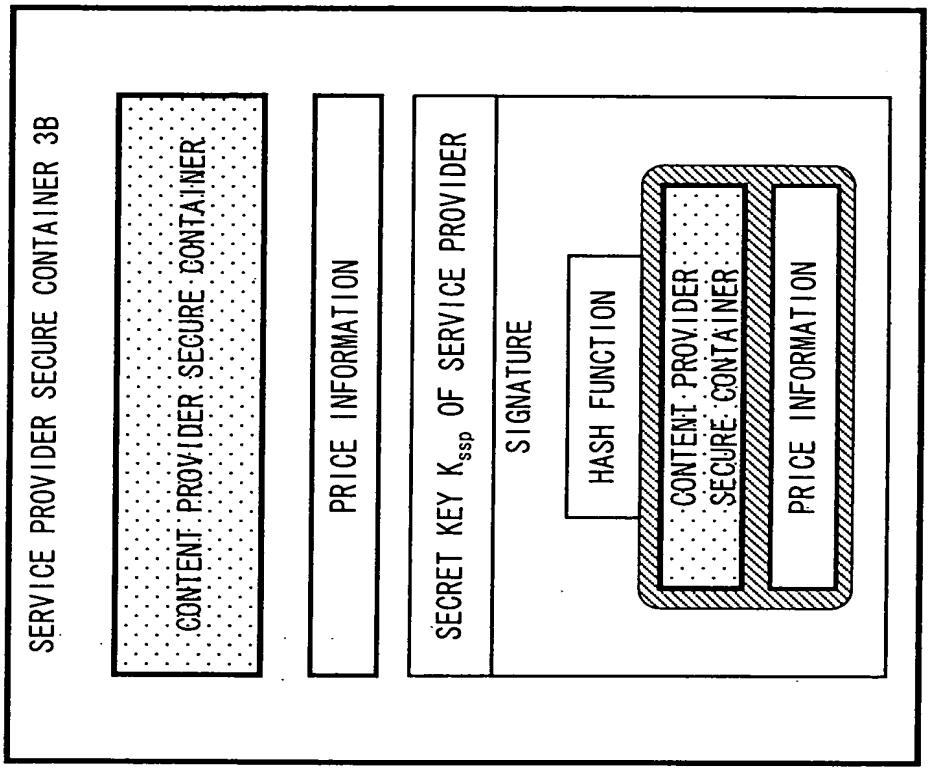
SERVICE PROVIDER SECURE CONTAINER 3B
CONTENT PROVIDER SECURE CONTAINER
PRICE INFORMATION
SECRET KEY K_{ssp} OF SERVICE PROVIDER
SIGNATURE
HASH FUNCTION
CONTENT PROVIDER SECURE CONTAINER
PRICE INFORMATION

FIG. 30

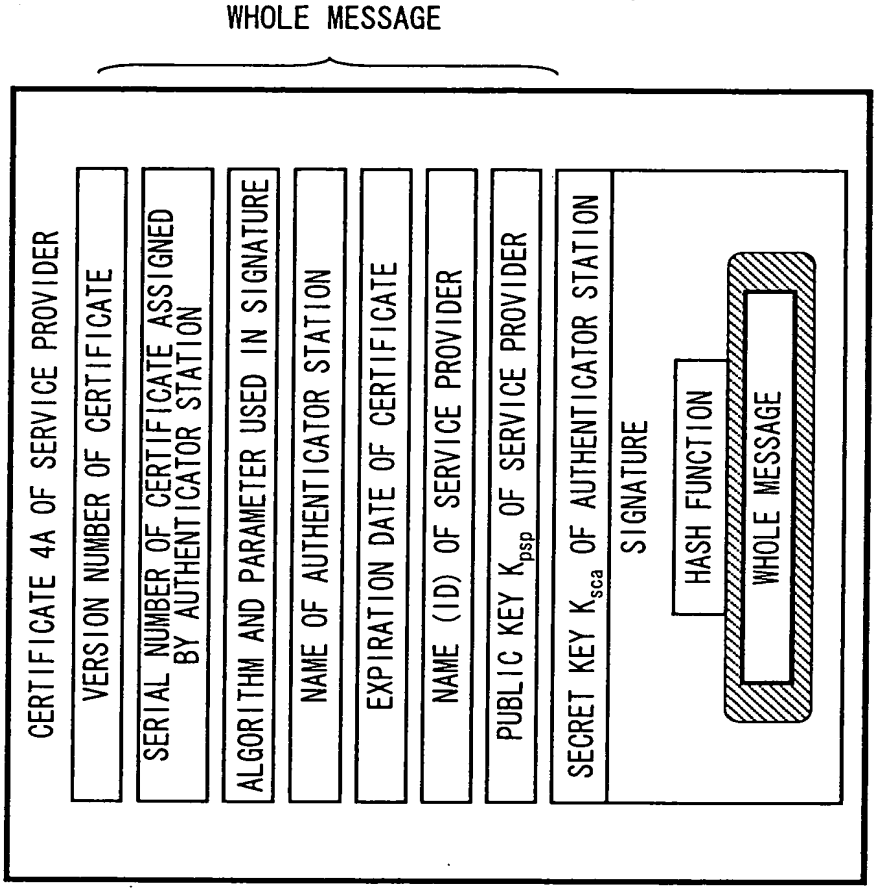
WHOLE MESSAGE
CERTIFICATE 4A OF SERVICE PROVIDER
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ASSIGNED BY AUTHENTICATOR STATION
ALGORITHM AND PARAMETER USED IN SIGNATURE
NAME OF AUTHENTICATOR STATION
EXPIRATION DATE OF CERTIFICATE
NAME (ID) OF SERVICE PROVIDER
PUBLIC KEY K_{psp} OF SERVICE PROVIDER
SECRET KEY K_{sca} OF AUTHENTICATOR STATION
SIGNATURE
HASH FUNCTION
WHOLE MESSAGE

FIG. 31

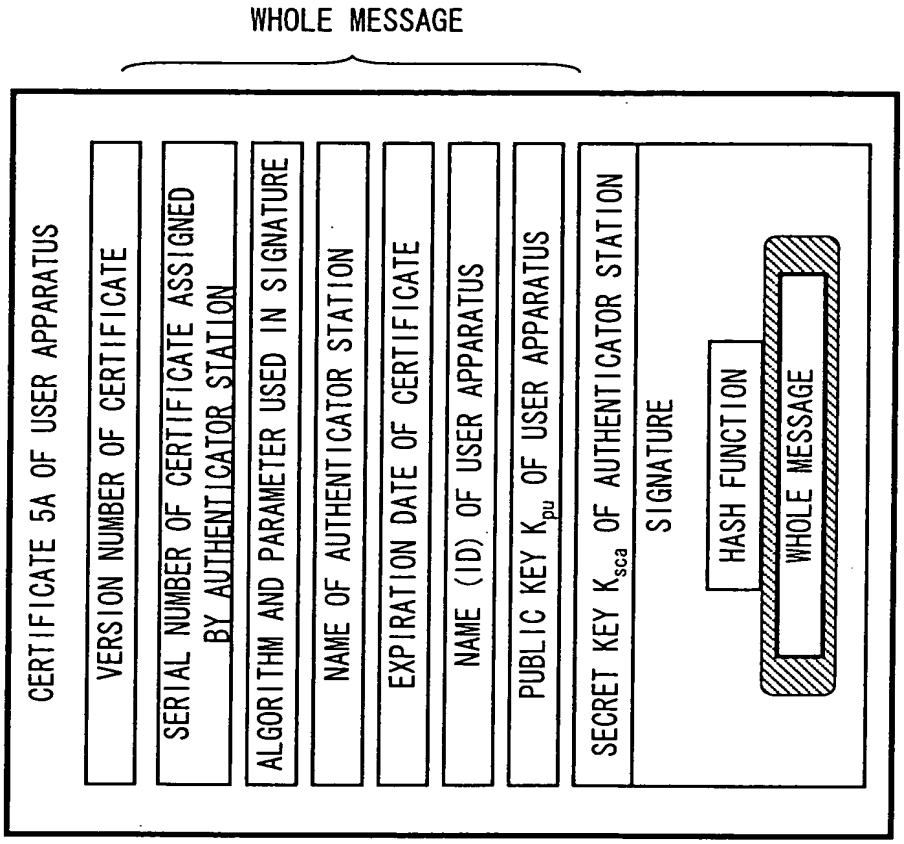
WHOLE MESSAGE
CERTIFICATE 5A OF USER APPARATUS
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ASSIGNED BY AUTHENTICATOR STATION
ALGORITHM AND PARAMETER USED IN SIGNATURE
NAME OF AUTHENTICATOR STATION
EXPIRATION DATE OF CERTIFICATE
NAME (ID) OF USER APPARATUS
PUBLIC KEY K_{pu} OF USER APPARATUS
SECRET KEY K_{sca} OF AUTHENTICATOR STATION
SIGNATURE
HASH FUNCTION
WHOLE MESSAGE

FIG. 32

TYPE OF DATA		
TYPE OF HANDLING POLICY (SINGLE)		
EXPIRATION DATE OF HANDLING POLICY		
ID OF CONTENTS		
ID OF CONTENT PROVIDER		
ID OF HANDLING POLICY		
VERSION OF HANDLING POLICY		
AREA CODE		
USAGE POSSIBLE APPARATUS CONDITION		
USAGE POSSIBLE USER CONDITION		
ID OF SERVICE PROVIDER		
GENERATION MANAGEMENT INFORMATION		
THE NUMBER OF RULES		
ADDRESS INFORMATION OF RULES		
RULE 1	RULE NUMBER (RULE #)	
	USAGE RIGHT CONTENT NUMBER (TYPE)	
	PARAMETER	
	MINIMUM SELLING-PRICE	
	AMOUNT OF BENEFITS OF CONTENT PROVIDER	
	RATE OF BENEFITS OF SERVICE PROVIDER	
	DATA SIZE	
	SENDING INFORMATION	
•••	•••	
RULE N	RULE NUMBER (RULE #)	
	USAGE RIGHT CONTENT NUMBER (TYPE)	
	PARAMETER	
	MINIMUM SELLING-PRICE	
	AMOUNT OF BENEFITS OF CONTENT PROVIDER	
	RATE OF BENEFITS OF SERVICE PROVIDER	
	DATA SIZE	
	SENDING INFORMATION	
(PRESENCE OR ABSENCE OF VERIFICATION OF SIGNATURE)		
PUBLIC KEY CERTIFICATE		
SIGNATURE		

FIG. 33

TYPE OF DATA	
TYPE OF HANDLING POLICY (ALBUM)	
EXPIRATION DATE OF HANDLING POLICY	
ID OF ALBUM	
VERSION OF HANDLING POLICY	
ID OF CONTENT PROVIDER	
ID OF HANDLING POLICY	
AREA CODE	
USAGE POSSIBLE APPARATUS CONDITION	
USAGE POSSIBLE USER CONDITION	
ID OF SERVICE PROVIDER	
NUMBER OF HANDLING POLICIES OF SINGLE CONTENTS	
ADDRESS INFORMATION OF HANDLING POLICY OF SINGLE CONTENTS	
SINGLE	HANDLING POLICY 1
	⋮
	HANDLING POLICY N
GENERATION MANAGEMENT INFORMATION	
NUMBER OF RULES	
ADDRESS INFORMATION OF RULES	
RULE 1	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	AMOUNT OF BENEFITS OF CONTENT PROVIDER
	RATE OF BENEFITS OF SERVICE PROVIDER
	DATA SIZE
	SENDING INFORMATION
⋮	⋮
RULE N	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	AMOUNT OF BENEFITS OF CONTENT PROVIDER
	RATE OF BENEFITS OF SERVICE PROVIDER
	DATA SIZE
	SENDING INFORMATION
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 34

TYPE OF DATA	
TYPE OF HANDLING POLICY (SINGLE)	
EXPIRATION DATE OF HANDLING POLICY	
ID OF CONTENTS	
ID OF CONTENT PROVIDER	
ID OF HANDLING POLICY	
VERSION OF HANDLING POLICY	
AREA CODE	
USAGE POSSIBLE APPARATUS CONDITION	
USAGE POSSIBLE USER CONDITION	
ID OF SERVICE PROVIDER	
GENERATION MANAGEMENT INFORMATION	
THE NUMBER OF RULES	
ADDRESS INFORMATION OF RULES	
RULE 1	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	DATA SIZE
	SENDING INFORMATION
• • •	• • •
RULE N	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	DATA SIZE
	SENDING INFORMATION
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 35

TYPE OF DATA	
TYPE OF HANDLING POLICY (ALBUM)	
EXPIRATION DATE OF HANDLING POLICY	
ID OF ALBUM	
VERSION OF HANDLING POLICY	
ID OF CONTENT PROVIDER	
ID OF HANDLING POLICY	
AREA CODE	
USAGE POSSIBLE APPARATUS CONDITION	
USAGE POSSIBLE USER CONDITION	
ID OF SERVICE PROVIDER	
NUMBER OF HANDLING POLICIES OF SINGLE CONTENTS	
ADDRESS INFORMATION OF HANDLING POLICY OF SINGLE CONTENTS	
SINGLE	HANDLING POLICY 1
	⋮
	HANDLING POLICY N
GENERATION MANAGEMENT INFORMATION	
NUMBER OF RULES	
ADDRESS INFORMATION OF RULES	
RULE 1	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	DATA SIZE
	SENDING INFORMATION
⋮	⋮
RULE N	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	DATA SIZE
	SENDING INFORMATION
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 36

TYPE OF DATA		
TYPE OF PRICE INFORMATION (SINGLE)		
EXPIRATION DATE OF PRICE INFORMATION		
ID OF CONTENTS		
ID OF SERVICE PROVIDER		
ID OF PRICE INFORMATION		
VERSION OF PRICE INFORMATION		
AREA CODE		
USAGE POSSIBLE APPARATUS CONDITION		
USAGE POSSIBLE USER CONDITION		
ID OF CONTENT PROVIDER		
ID OF HANDLING POLICY		
NUMBER OF RULES		
ADDRESS INFORMATION OF RULES		
RULE 1	RULE NUMBER (RULE#)	
	AMOUNT OF BENEFITS OF SERVICE PROVIDER	
	RATE OF BENEFITS OF SERVICE PROVIDER	
	PRICE	
	DATA SIZE	
	SENDING INFORMATION	
•••	•••	
RULE N	RULE NUMBER (RULE#)	
	AMOUNT OF BENEFITS OF SERVICE PROVIDER	
	RATE OF BENEFITS OF SERVICE PROVIDER	
	PRICE	
	DATA SIZE	
	SENDING INFORMATION	
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)		
PUBLIC KEY CERTIFICATE		
SIGNATURE		

FIG. 37

TYPE OF DATA		
TYPE OF PRICE INFORMATION (ALBUM)		
EXPIRATION DATE OF PRICE INFORMATION		
ID OF ALBUM		
ID OF SERVICE PROVIDER		
ID OF PRICE INFORMATION		
VERSION OF PRICE INFORMATION		
AREA CODE		
USAGE POSSIBLE APPARATUS CONDITION		
USAGE POSSIBLE USER CONDITION		
ID OF CONTENT PROVIDER		
ID OF HANDLING POLICY		
NUMBER OF PRICE INFORMATION OF SINGLE CONTENTS		
ADDRESS INFORMATION OF PRICE INFORMATION OF SINGLE CONTENTS		
SINGLE	PRICE INFORMATION 1	
	• • •	
	PRICE INFORMATION N	
NUMBER OF RULES		
ADDRESS INFORMATION OF RULES		
RULE 1	RULE NUMBER (RULE#)	
	AMOUNT OF BENEFITS OF SERVICE PROVIDER	
	RATE OF BENEFITS OF SERVICE PROVIDER	
	PRICE	
	DATA SIZE	
	SENDING INFORMATION	
• • •	• • •	
RULE N	RULE NUMBER (RULE#)	
	AMOUNT OF BENEFITS OF SERVICE PROVIDER	
	RATE OF BENEFITS OF SERVICE PROVIDER	
	PRICE	
	DATA SIZE	
	SENDING INFORMATION	
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)		
PUBLIC KEY CERTIFICATE		
SIGNATURE		

FIG. 38

TYPE OF DATA		
TYPE OF PRICE INFORMATION (SINGLE)		
EXPIRATION DATE OF PRICE INFORMATION		
ID OF CONTENTS		
ID OF SERVICE PROVIDER		
ID OF PRICE INFORMATION		
VERSION OF PRICE INFORMATION		
AREA CODE		
USAGE POSSIBLE APPARATUS CONDITION		
USAGE POSSIBLE USER CONDITION		
ID OF CONTENT PROVIDER		
ID OF HANDLING POLICY		
NUMBER OF RULES		
ADDRESS INFORMATION OF RULES		
RULE 1	RULE NUMBER (RULE#)	
	PRICE	
	DATA SIZE	
	SENDING INFORMATION	
•••	⋮	
RULE N	RULE NUMBER (RULE#)	
	PRICE	
	DATA SIZE	
	SENDING INFORMATION	
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)		
PUBLIC KEY CERTIFICATE		
SIGNATURE		

FIG. 39

TYPE OF DATA		
TYPE OF PRICE INFORMATION (ALBUM)		
EXPIRATION DATE OF PRICE INFORMATION		
ID OF ALBUM		
ID OF SERVICE PROVIDER		
ID OF PRICE INFORMATION		
VERSION OF PRICE INFORMATION		
AREA CODE		
USAGE POSSIBLE APPARATUS CONDITION		
USAGE POSSIBLE USER CONDITION		
ID OF CONTENT PROVIDER		
ID OF HANDLING POLICY		
NUMBER OF PRICE INFORMATION OF SINGLE CONTENTS		
ADDRESS INFORMATION OF PRICE INFORMATION OF SINGLE CONTENTS		
SINGLE	PRICE INFORMATION 1	
	⋮	
	PRICE INFORMATION N	
NUMBER OF RULES		
ADDRESS INFORMATION OF RULES		
RULE 1	RULE NUMBER (RULE#)	
	PRICE	
	DATA SIZE	
	SENDING INFORMATION	
⋮	⋮	
RULE N	RULE NUMBER (RULE#)	
	PRICE	
	DATA SIZE	
	SENDING INFORMATION	
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)		
PUBLIC KEY CERTIFICATE		
SIGNATURE		

FIG. 40

TYPE OF DATA
TYPE OF LICENSE CONDITION INFORMATION
EXPIRATION DATE OF LICENSE CONDITION INFORMATION
ID OF CONTENTS
ID OF ALBUM
ID OF CIPHER PROCESSING PORTION
ID OF USER
ID OF CONTENT PROVIDER
ID OF HANDLING POLICY
VERSION OF HANDLING POLICY
ID OF SERVICE PROVIDER
ID OF PRICE INFORMATION
VERSION OF PRICE INFORMATION
ID OF LICENSE CONDITION INFORMATION
RULE NUMBER OF PLAYBACK RIGHT (USAGE RIGHT)
USAGE RIGHT CONTENT NUMBER
REMAINING NUMBER OF TIMES OF PLAYBACK
EXPIRATION DATE OF PLAYBACK RIGHT
RULE NUMBER OF REPLICATION RIGHT(USAGE RIGHT)
USAGE RIGHT CONTENT NUMBER
REMAINING NUMBER OF TIMES OF REPLICATION
GENERATION MANAGEMENT INFORMATION
ID OF CIPHER PROCESSING PORTION POSSESSING PLAYBACK RIGHT

09830392.061801

FIG. 41

TYPE OF DATA
ID OF CIPHER PROCESSING PORTION
ID OF USER
ID OF CONTENTS
ID OF CONTENT PROVIDER
ID OF HANDLING POLICY
VERSION OF HANDLING POLICY
ID OF SERVICE PROVIDER
ID OF PRICE INFORMATION
VERSION OF PRICE INFORMATION
ID OF LICENSE CONDITION INFORMATION
RULE NUMBER (RULE #)
AMOUNT / RATE OF BENEFITS OF CONTENT PROVIDER
AMOUNT / RATE OF BENEFITS OF SERVICE PROVIDER
GENERATION MANAGEMENT INFORMATION
DATA SIZE OF SENDING INFORMATION DEFINED BY CONTENT PROVIDER
SENDING INFORMATION DEFINED BY CONTENT PROVIDER
DATA SIZE OF SENDING INFORMATION DEFINED BY SERVICE PROVIDER
SENDING INFORMATION DEFINED BY SERVICE PROVIDER
ID OF SUPPLIER

FIG. 42

TYPE OF DATA
ID OF CIPHER PROCESSING PORTION
ID OF USER
ID OF CONTENTS
ID OF CONTENT PROVIDER
ID OF HANDLING POLICY
VERSION OF HANDLING POLICY
ID OF SERVICE PROVIDER
ID OF PRICE INFORMATION
VERSION OF PRICE INFORMATION
ID OF LICENSE CONDITION INFORMATION
RULE NUMBER (RULE #)
GENERATION MANAGEMENT INFORMATION
DATA SIZE OF SENDING INFORMATION DEFINED BY CONTENT PROVIDER
SENDING INFORMATION DEFINED BY CONTENT PROVIDER
DATA SIZE OF SENDING INFORMATION DEFINED BY SERVICE PROVIDER
SENDING INFORMATION DEFINED BY SERVICE PROVIDER
ID OF SUPPLIER

FIG. 43

USAGE RIGHT CONTENT NUMBER	USAGE RIGHT CONTENT			
	RIGHT	LIMIT ON PERIOD	LIMIT ON THE NUMBER OF TIMES	LIMIT ON REPLICATION
(1)	PLAYBACK RIGHT	NOT IMPOSED	NOT IMPOSED	—
(2)		IMPOSED	NOT IMPOSED	—
(3)		IMPOSED	NOT IMPOSED	—
(4)		NOT IMPOSED	IMPOSED	—
(5)	REPLICATION RIGHT	NOT IMPOSED	NOT IMPOSED	NOT IMPOSED
(6)		NOT IMPOSED	IMPOSED	NOT IMPOSED
(7)		NOT IMPOSED	NOT IMPOSED	SCMS
(8)		NOT IMPOSED	IMPOSED	
(9) ~ (15)	SPARES			
(16)	RIGHT TO CHANGE RIGHT CONTENTS	—		
(17)	REPURCHASE RIGHT	—		
(18)	ADDITIONAL PURCHASE RIGHT	—		
(19)	MANAGEMENT TRANSFER RIGHT	—		

FIG. 44

09/830392

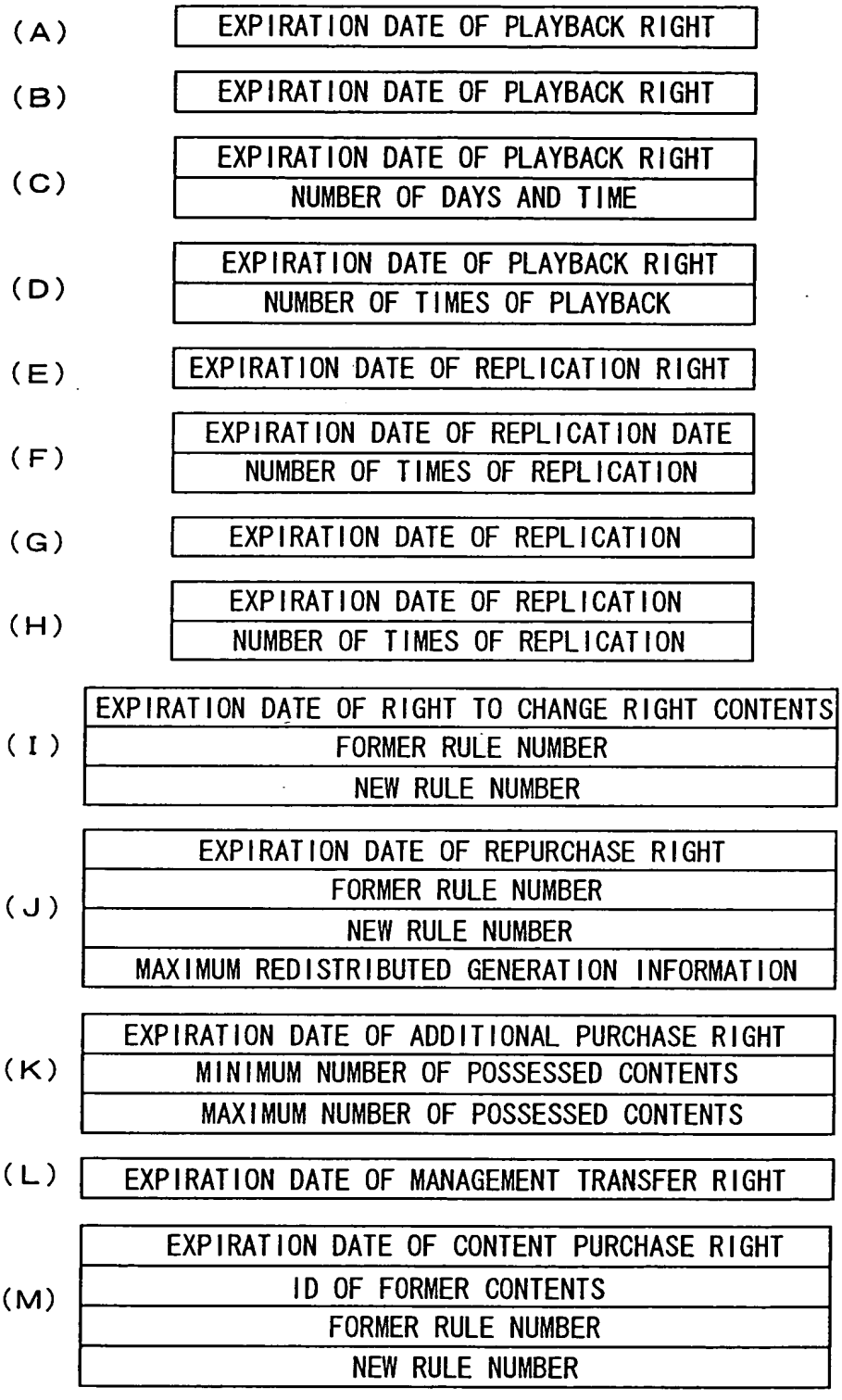

FIG. 45

EP0954850A1

TYPE OF DATA
TYPE OF CONTENTS (SINGLE)
EXPIRATION DATE OF CONTENTS
CATEGORY OF CONTENTS
ID OF CONTENTS
ID OF CONTENT PROVIDER
CRYPTOSYSTEM OF CONTENTS
DATA LENGTH OF ENCRYPTED CONTENTS
ENCRYPTED CONTENTS
PUBLIC KEY CERTIFICATE
SIGNATURE

FIG. 46

TYPE OF DATA	
TYPE OF CONTENTS (ALBUM)	
EXPIRATION DATE OF CONTENTS	
ID OF ALBUM	
ID OF CONTENT PROVIDER	
NUMBER OF SINGLE CONTENTS	
ADDRESS INFORMATION OF SINGLE CONTENTS	
SINGLE	CONTENTS 1
	⋮
	CONTENTS N
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 47

09830392.061801

TYPE OF DATA
TYPE OF KEY DATA (SINGLE)
EXPIRATION DATE OF KEY
ID OF CONTENTS
ID OF CONTENT PROVIDER
KEY VERSION
CRYPTOSYSTEM OF CONTENT KEY
ENCRYPTED CONTENT KEY
CRYPTOSYSTEM OF INDIVIDUAL KEY
ENCRYPTED INDIVIDUAL KEY
PUBLIC KEY CERTIFICATE
SIGNATURE

09830392 . 061801

FIG. 48

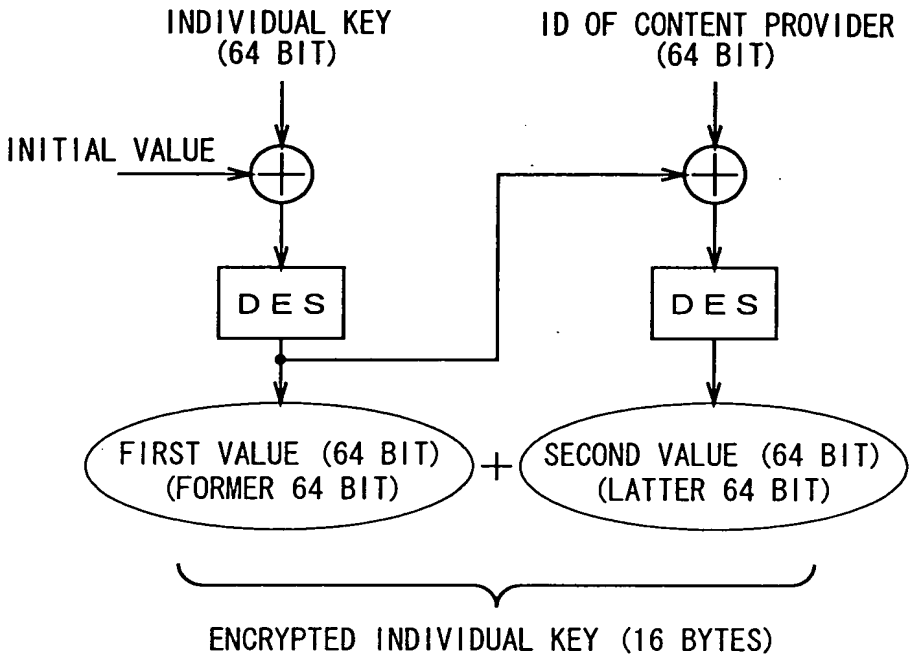
INDIVIDUAL KEY
(64 BIT)
ID OF CONTENT PROVIDER
(64 BIT)
INITIAL VALUE
DES
DES
FIRST VALUE (64 BIT)
(FORMER 64 BIT)
+
SECOND VALUE (64 BIT)
(LATTER 64 BIT)
ENCRYPTED INDIVIDUAL KEY (16 BYTES)

FIG. 49

EP0763950A1

TYPE OF DATA	
TYPE OF KEY DATA (ALBUM)	
EXPIRATION DATE OF KEY	
ID OF ALBUM	
CONTENT PROVIDER ID	
VERSION OF KEY	
NUMBER OF KEY DATA FOR SINGLE CONTENTS	
ADDRESS INFORMATION OF KEY DATA FOR SINGLE CONTENTS	
SINGLE	KEY DATA 1
	⋮
	KEY DATA N
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 50

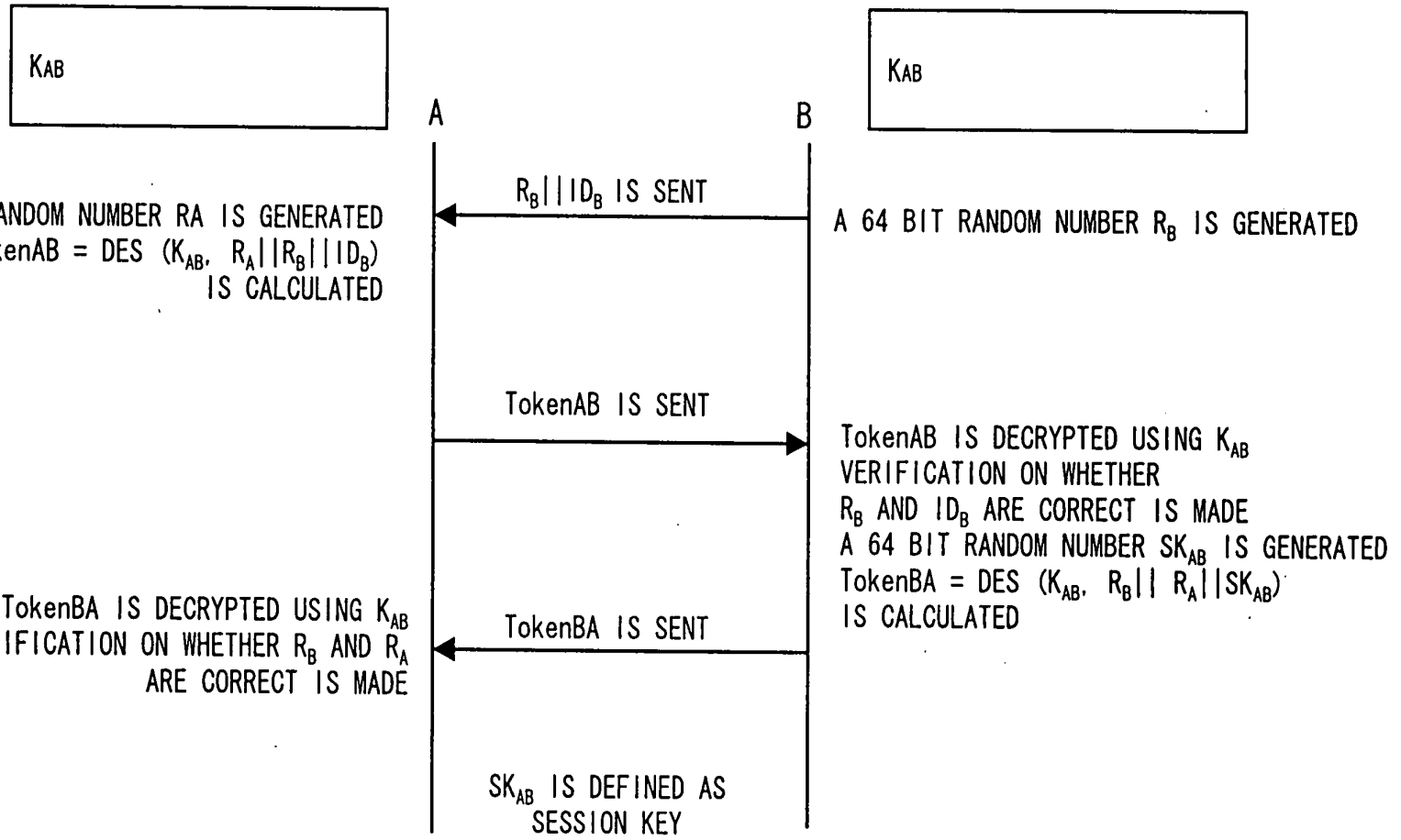
KAB
KAB
A
B
A 64 BIT RANDOM NUMBER RA IS GENERATED
TokenAB = DES (KAB, RA||RB|||IDB)
IS CALCULATED
RB|||IDB IS SENT
A 64 BIT RANDOM NUMBER RB IS GENERATED
TokenAB IS SENT
TokenAB IS DECRYPTED USING KAB
VERIFICATION ON WHETHER
RB AND IDB ARE CORRECT IS MADE
A 64 BIT RANDOM NUMBER SKAB IS GENERATED
TokenBA = DES (KAB, RB|| RA||SKAB)
IS CALCULATED
TokenBA IS DECRYPTED USING KAB
VERIFICATION ON WHETHER RB AND RA
ARE CORRECT IS MADE
TokenBA IS SENT
SKAB IS DEFINED AS
SESSION KEY

FIG. 51

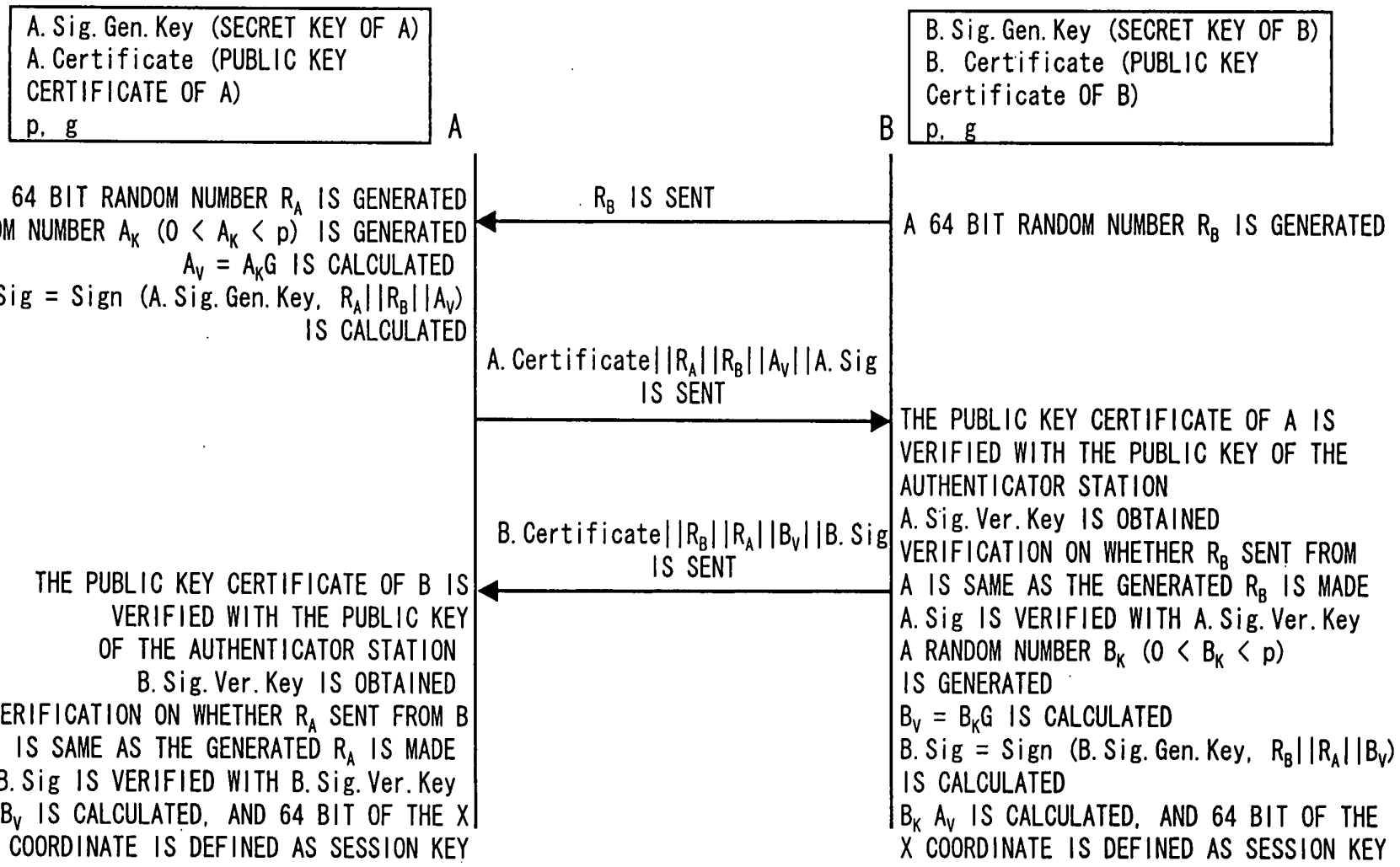
A. Sig. Gen. Key (SECRET KEY OF A)
A. Certificate (PUBLIC KEY CERTIFICATE OF A)
p, g
A
B
B. Sig. Gen. Key (SECRET KEY OF B)
B. Certificate (PUBLIC KEY Certificate OF B)
p, g
A 64 BIT RANDOM NUMBER R_A IS GENERATED
A RANDOM NUMBER A_K ($0 < A_K < p$) IS GENERATED
$A_V = A_K G$ IS CALCULATED
A. Sig = Sign (A. Sig. Gen. Key, $R_A||R_B||A_V$) IS CALCULATED
R_B IS SENT
A 64 BIT RANDOM NUMBER R_B IS GENERATED
A. Certificate$||R_A||R_B||A_V||$A. Sig IS SENT
THE PUBLIC KEY CERTIFICATE OF A IS VERIFIED WITH THE PUBLIC KEY OF THE AUTHENTICATOR STATION
A. Sig. Ver. Key IS OBTAINED
VERIFICATION ON WHETHER R_B SENT FROM A IS SAME AS THE GENERATED R_B IS MADE
A. Sig IS VERIFIED WITH A. Sig. Ver. Key
A RANDOM NUMBER B_K ($0 < B_K < p$) IS GENERATED
$B_V = B_K G$ IS CALCULATED
B. Sig = Sign (B. Sig. Gen. Key, $R_B||R_A||B_V$) IS CALCULATED
$B_K A_V$ IS CALCULATED, AND 64 BIT OF THE X COORDINATE IS DEFINED AS SESSION KEY
B. Certificate$||R_B||R_A||B_V||$B. Sig IS SENT
THE PUBLIC KEY CERTIFICATE OF B IS VERIFIED WITH THE PUBLIC KEY OF THE AUTHENTICATOR STATION
B. Sig. Ver. Key IS OBTAINED
VERIFICATION ON WHETHER R_A SENT FROM B IS SAME AS THE GENERATED R_A IS MADE
B. Sig IS VERIFIED WITH B. Sig. Ver. Key
$A_K B_V$ IS CALCULATED, AND 64 BIT OF THE X COORDINATE IS DEFINED AS SESSION KEY

FIG. 52

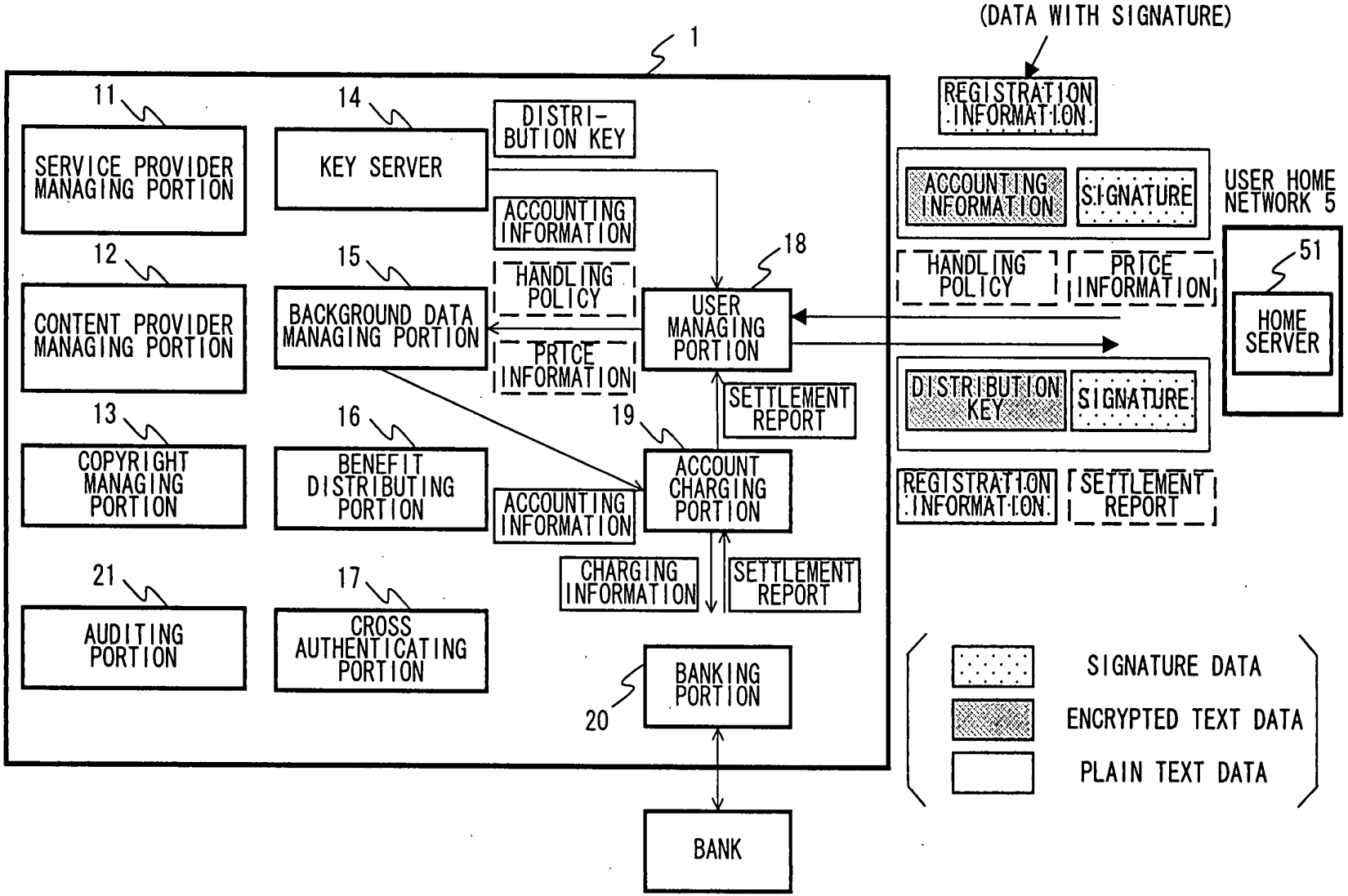
(DATA WITH SIGNATURE)
1
11
SERVICE PROVIDER MANAGING PORTION
12
CONTENT PROVIDER MANAGING PORTION
13
COPYRIGHT MANAGING PORTION
21
AUDITING PORTION
14
KEY SERVER
15
BACKGROUND DATA MANAGING PORTION
16
BENEFIT DISTRIBUTING PORTION
17
CROSS AUTHENTICATING PORTION
DISTRI-BUTION KEY
ACCOUNTING INFORMATION
HANDLING POLICY
PRICE INFORMATION
18
USER MANAGING PORTION
SETTLEMENT REPORT
19
ACCOUNT CHARGING PORTION
ACCOUNTING INFORMATION
CHARGING INFORMATION
SETTLEMENT REPORT
20
BANKING PORTION
BANK
REGISTRATION INFORMATION
ACCOUNTING INFORMATION
SIGNATURE
HANDLING POLICY
PRICE INFORMATION
DISTRIBUTION KEY
SIGNATURE
REGISTRATION INFORMATION
SETTLEMENT REPORT
USER HOME NETWORK 5
51
HOME SERVER
SIGNATURE DATA
ENCRYPTED TEXT DATA
PLAIN TEXT DATA

FIG. 53

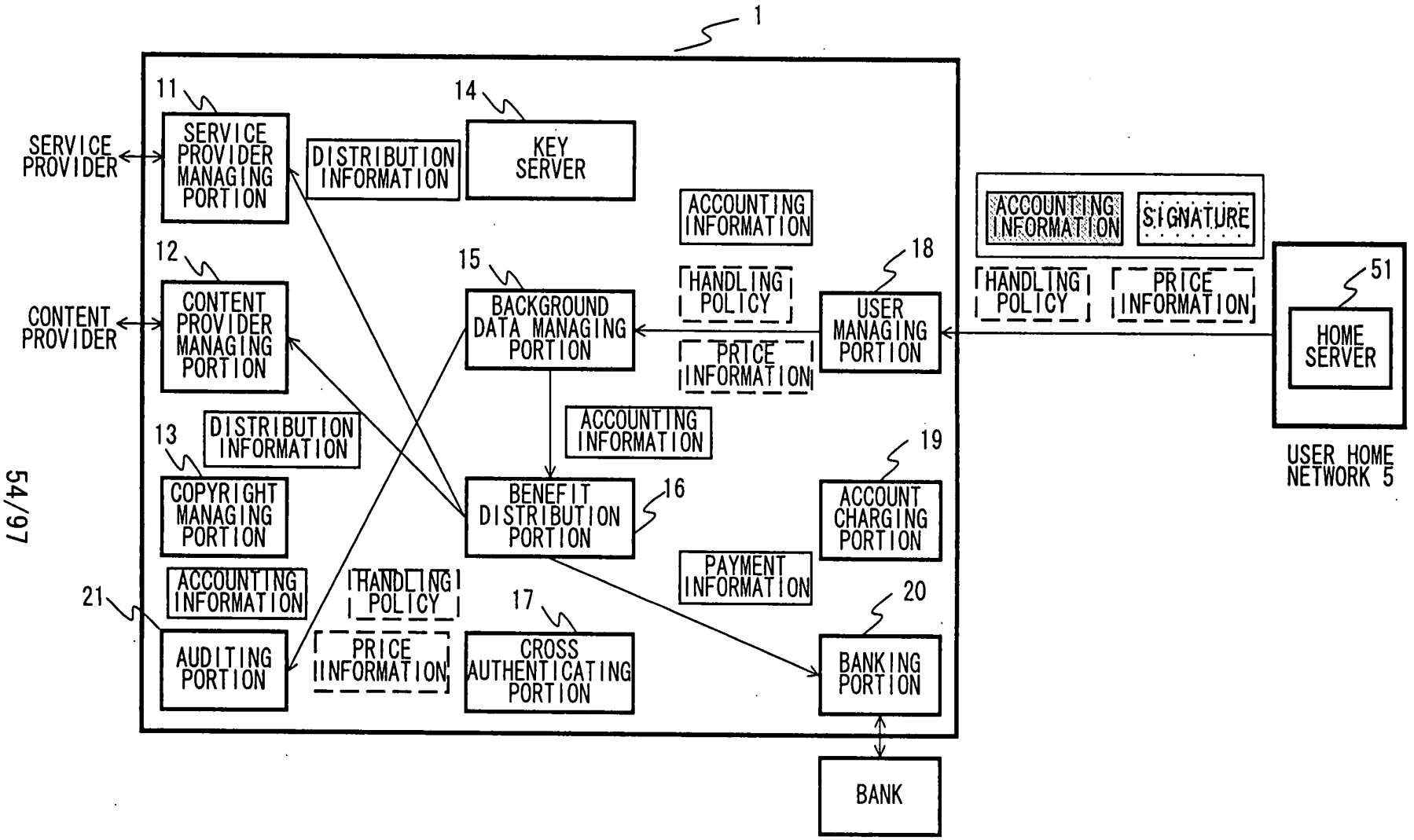
1
11
SERVICE PROVIDER MANAGING PORTION
SERVICE PROVIDER
DISTRIBUTION INFORMATION
14
KEY SERVER
12
CONTENT PROVIDER MANAGING PORTION
CONTENT PROVIDER
15
BACKGROUND DATA MANAGING PORTION
ACCOUNTING INFORMATION
HANDLING POLICY
PRTCE INFORMATION
18
USER MANAGING PORTION
ACCOUNTING INFORMATION
SIGNATURE
HANDLING POLICY
PRICE INFORMATION
51
HOME SERVER
USER HOME NETWORK 5
13
DISTRIBUTION INFORMATION
COPYRIGHT MANAGING PORTION
ACCOUNTING INFORMATION
BENEFIT DISTRIBUTION PORTION
16
19
ACCOUNT CHARGING PORTION
PAYMENT INFORMATION
21
AUDITING PORTION
HANDLING POLICY
PRICE INFORMATION
17
CROSS AUTHENTICATING PORTION
20
BANKING PORTION
BANK

FIG. 54

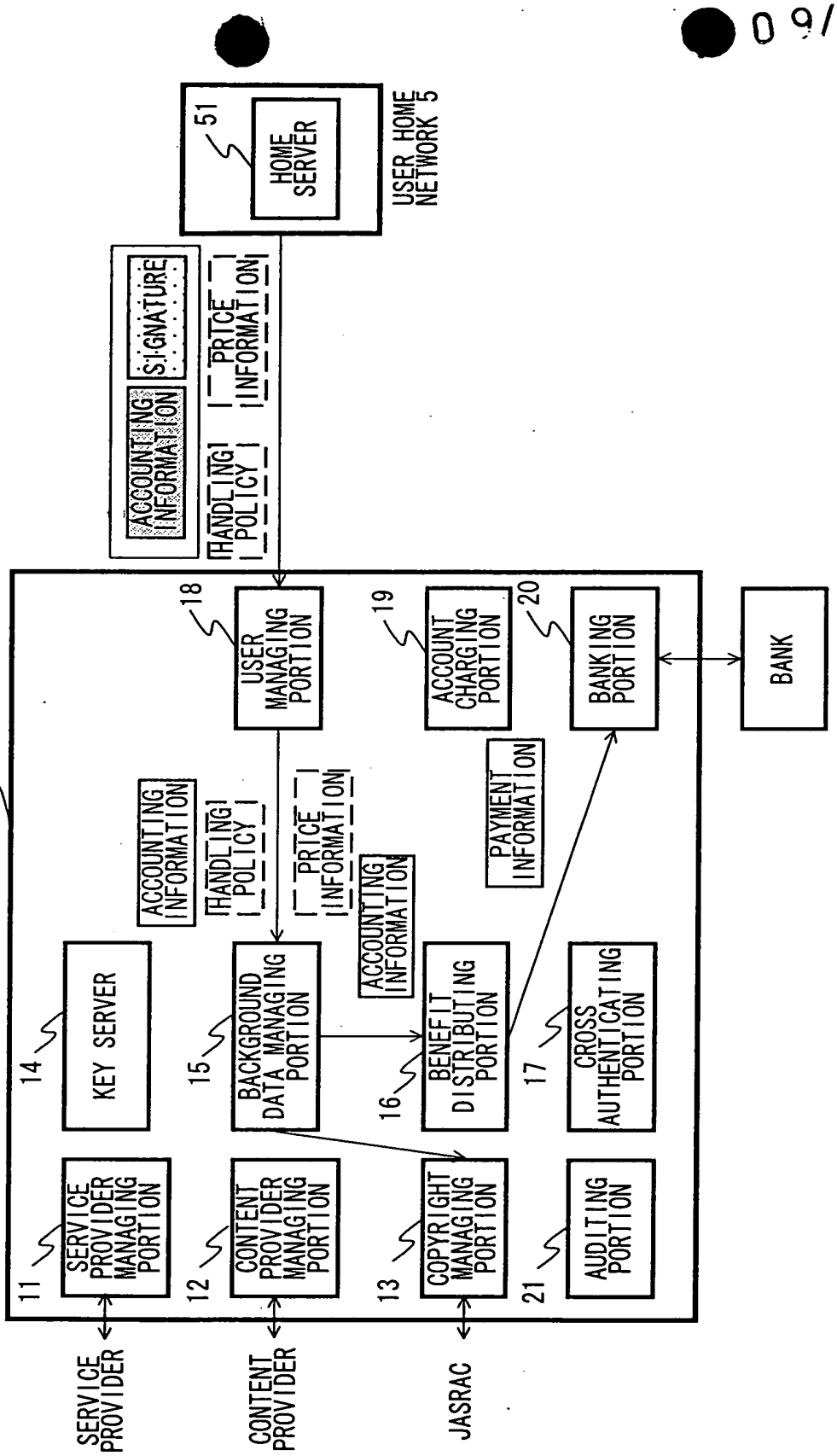
USER HOME NETWORK 5
51
HOME SERVER
ACCOUNTING INFORMATION
SIGNATURE
HANDLING POLICY
PRICE INFORMATION
1
18
USER MANAGING PORTION
19
ACCOUNT CHARGING PORTION
20
BANKING PORTION
BANK
ACCOUNTING INFORMATION
HANDLING POLICY
PRICE INFORMATION
ACCOUNTING INFORMATION
PAYMENT INFORMATION
14
KEY SERVER
15
BACKGROUND DATA MANAGING PORTION
16
BENEFIT DISTRIBUTING PORTION
17
CROSS AUTHENTICATING PORTION
11
SERVICE PROVIDER MANAGING PORTION
12
CONTENT PROVIDER MANAGING PORTION
13
COPYRIGHT MANAGING PORTION
21
AUDITING PORTION
SERVICE PROVIDER
CONTENT PROVIDER
JASRAC

FIG. 55

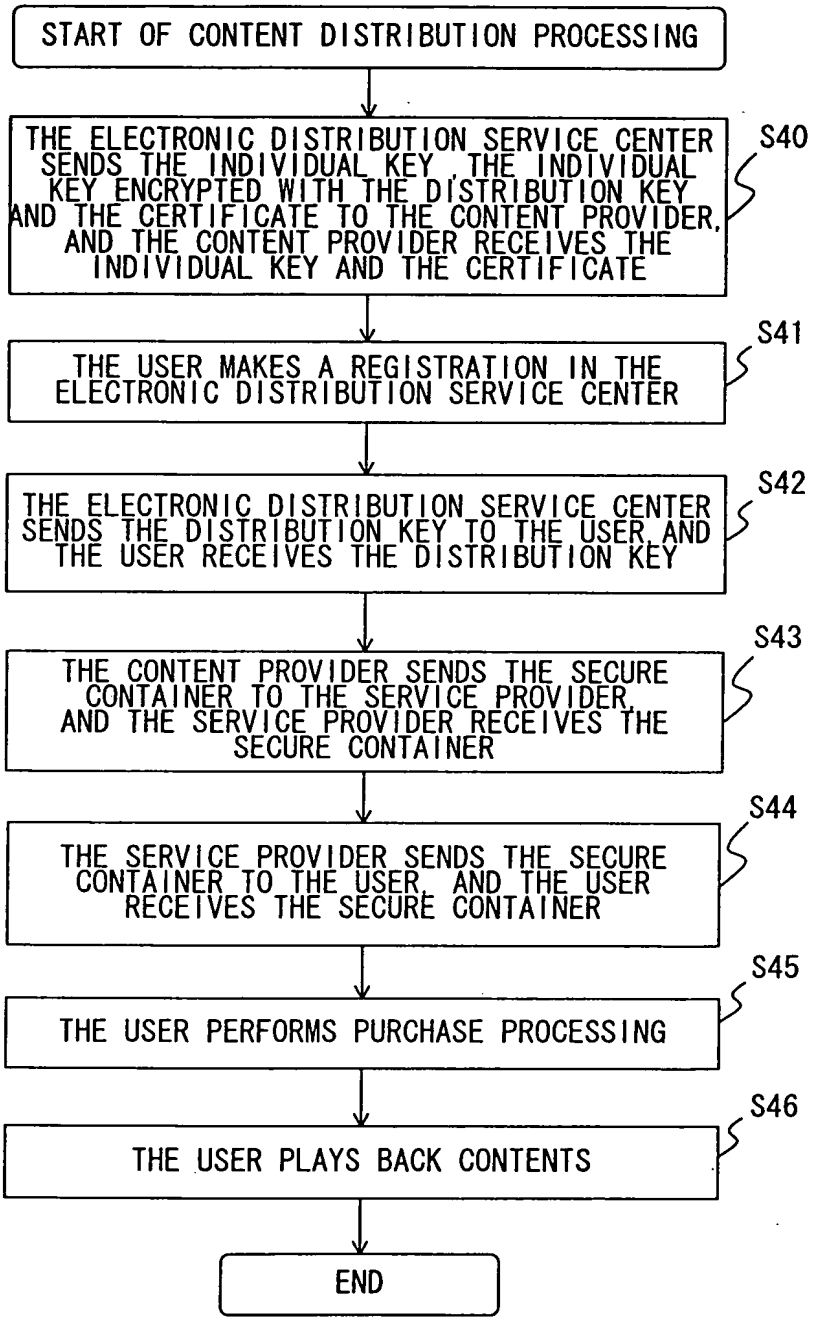
START OF CONTENT DISTRIBUTION PROCESSING
THE ELECTRONIC DISTRIBUTION SERVICE CENTER SENDS THE INDIVIDUAL KEY, THE INDIVIDUAL KEY ENCRYPTED WITH THE DISTRIBUTION KEY AND THE CERTIFICATE TO THE CONTENT PROVIDER, AND THE CONTENT PROVIDER RECEIVES THE INDIVIDUAL KEY AND THE CERTIFICATE
S40
THE USER MAKES A REGISTRATION IN THE ELECTRONIC DISTRIBUTION SERVICE CENTER
S41
THE ELECTRONIC DISTRIBUTION SERVICE CENTER SENDS THE DISTRIBUTION KEY TO THE USER AND THE USER RECEIVES THE DISTRIBUTION KEY
S42
THE CONTENT PROVIDER SENDS THE SECURE CONTAINER TO THE SERVICE PROVIDER, AND THE SERVICE PROVIDER RECEIVES THE SECURE CONTAINER
S43
THE SERVICE PROVIDER SENDS THE SECURE CONTAINER TO THE USER, AND THE USER RECEIVES THE SECURE CONTAINER
S44
THE USER PERFORMS PURCHASE PROCESSING
S45
THE USER PLAYS BACK CONTENTS
S46
END

FIG. 56

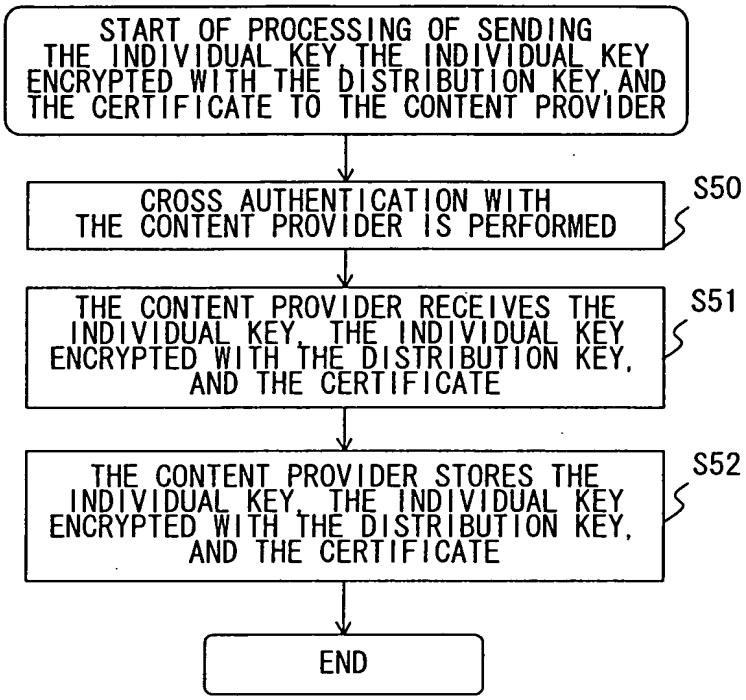
START OF PROCESSING OF SENDING THE INDIVIDUAL KEY, THE INDIVIDUAL KEY ENCRYPTED WITH THE DISTRIBUTION KEY, AND THE CERTIFICATE TO THE CONTENT PROVIDER
CROSS AUTHENTICATION WITH THE CONTENT PROVIDER IS PERFORMED
S50
THE CONTENT PROVIDER RECEIVES THE INDIVIDUAL KEY, THE INDIVIDUAL KEY ENCRYPTED WITH THE DISTRIBUTION KEY, AND THE CERTIFICATE
S51
THE CONTENT PROVIDER STORES THE INDIVIDUAL KEY, THE INDIVIDUAL KEY ENCRYPTED WITH THE DISTRIBUTION KEY, AND THE CERTIFICATE
S52
END

FIG. 57

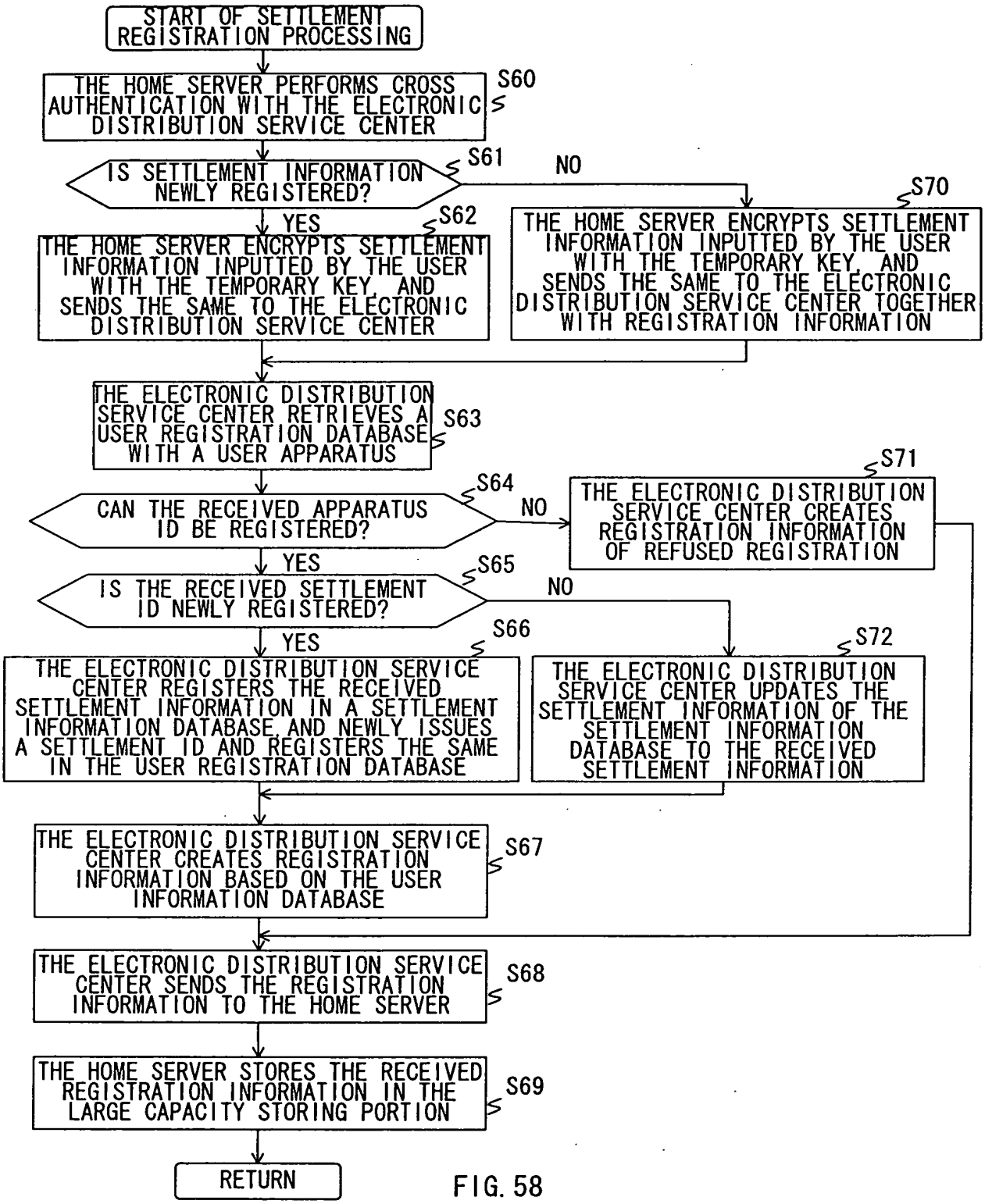
START OF SETTLEMENT REGISTRATION PROCESSING
THE HOME SERVER PERFORMS CROSS AUTHENTICATION WITH THE ELECTRONIC DISTRIBUTION SERVICE CENTER
S60
IS SETTLEMENT INFORMATION NEWLY REGISTERED?
S61
NO
YES
S62
THE HOME SERVER ENCRYPTS SETTLEMENT INFORMATION INPUTTED BY THE USER WITH THE TEMPORARY KEY, AND SENDS THE SAME TO THE ELECTRONIC DISTRIBUTION SERVICE CENTER
S70
THE HOME SERVER ENCRYPTS SETTLEMENT INFORMATION INPUTTED BY THE USER WITH THE TEMPORARY KEY, AND SENDS THE SAME TO THE ELECTRONIC DISTRIBUTION SERVICE CENTER TOGETHER WITH REGISTRATION INFORMATION
THE ELECTRONIC DISTRIBUTION SERVICE CENTER RETRIEVES A USER REGISTRATION DATABASE WITH A USER APPARATUS
S63
CAN THE RECEIVED APPARATUS ID BE REGISTERED?
S64
NO
S71
THE ELECTRONIC DISTRIBUTION SERVICE CENTER CREATES REGISTRATION INFORMATION OF REFUSED REGISTRATION
YES
IS THE RECEIVED SETTLEMENT ID NEWLY REGISTERED?
S65
NO
YES
S66
THE ELECTRONIC DISTRIBUTION SERVICE CENTER REGISTERS THE RECEIVED SETTLEMENT INFORMATION IN A SETTLEMENT INFORMATION DATABASE, AND NEWLY ISSUES A SETTLEMENT ID AND REGISTERS THE SAME IN THE USER REGISTRATION DATABASE
S72
THE ELECTRONIC DISTRIBUTION SERVICE CENTER UPDATES THE SETTLEMENT INFORMATION OF THE SETTLEMENT INFORMATION DATABASE TO THE RECEIVED SETTLEMENT INFORMATION
THE ELECTRONIC DISTRIBUTION SERVICE CENTER CREATES REGISTRATION INFORMATION BASED ON THE USER INFORMATION DATABASE
S67
THE ELECTRONIC DISTRIBUTION SERVICE CENTER SENDS THE REGISTRATION INFORMATION TO THE HOME SERVER
S68
THE HOME SERVER STORES THE RECEIVED REGISTRATION INFORMATION IN THE LARGE CAPACITY STORING PORTION
S69
RETURN

FIG. 58

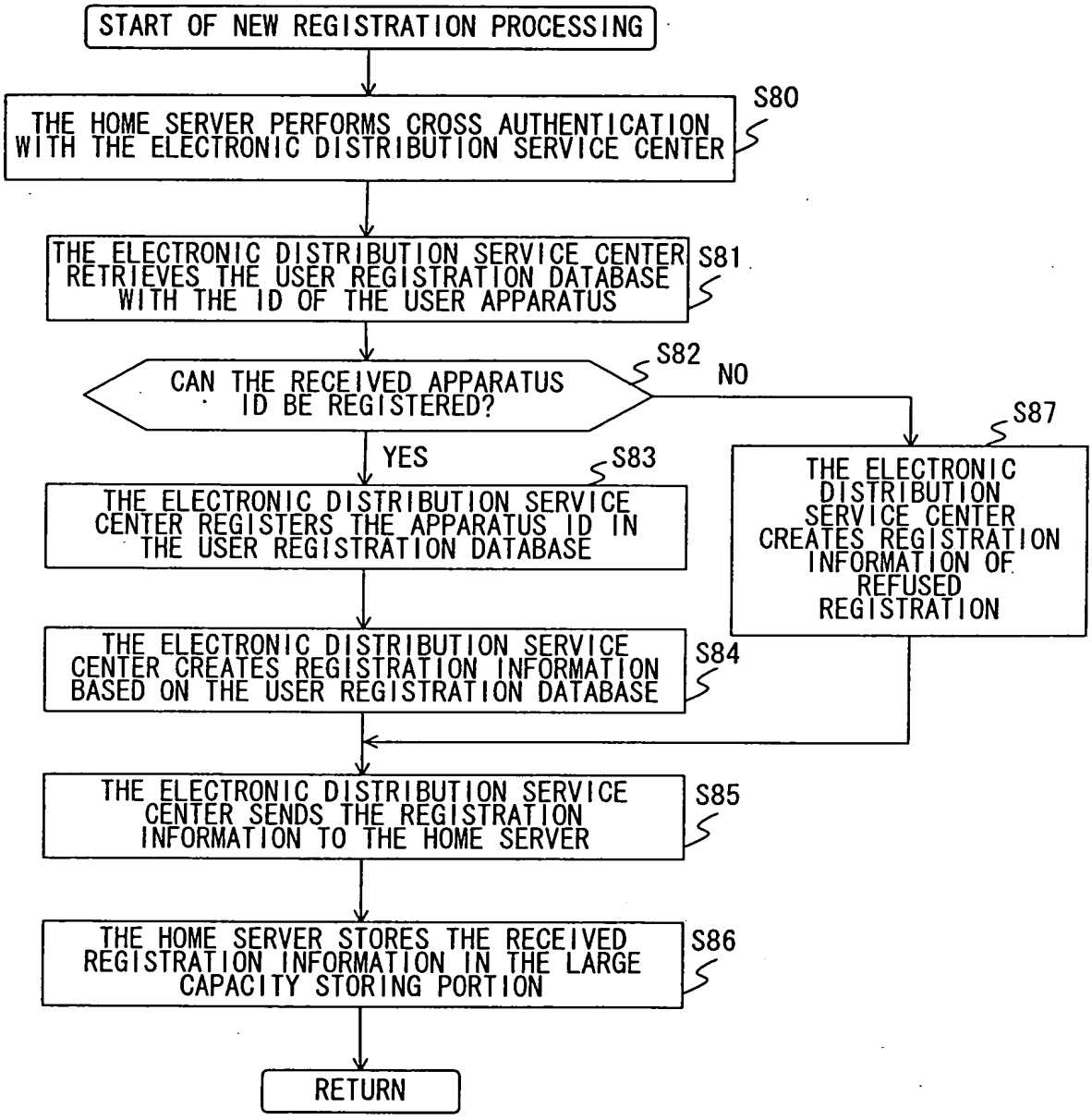
START OF NEW REGISTRATION PROCESSING
THE HOME SERVER PERFORMS CROSS AUTHENTICATION WITH THE ELECTRONIC DISTRIBUTION SERVICE CENTER
S80
THE ELECTRONIC DISTRIBUTION SERVICE CENTER RETRIEVES THE USER REGISTRATION DATABASE WITH THE ID OF THE USER APPARATUS
S81
CAN THE RECEIVED APPARATUS ID BE REGISTERED?
S82
NO
YES
S83
THE ELECTRONIC DISTRIBUTION SERVICE CENTER REGISTERS THE APPARATUS ID IN THE USER REGISTRATION DATABASE
S87
THE ELECTRONIC DISTRIBUTION SERVICE CENTER CREATES REGISTRATION INFORMATION OF REFUSED REGISTRATION
THE ELECTRONIC DISTRIBUTION SERVICE CENTER CREATES REGISTRATION INFORMATION BASED ON THE USER REGISTRATION DATABASE
S84
THE ELECTRONIC DISTRIBUTION SERVICE CENTER SENDS THE REGISTRATION INFORMATION TO THE HOME SERVER
S85
THE HOME SERVER STORES THE RECEIVED REGISTRATION INFORMATION IN THE LARGE CAPACITY STORING PORTION
S86
RETURN

FIG. 59

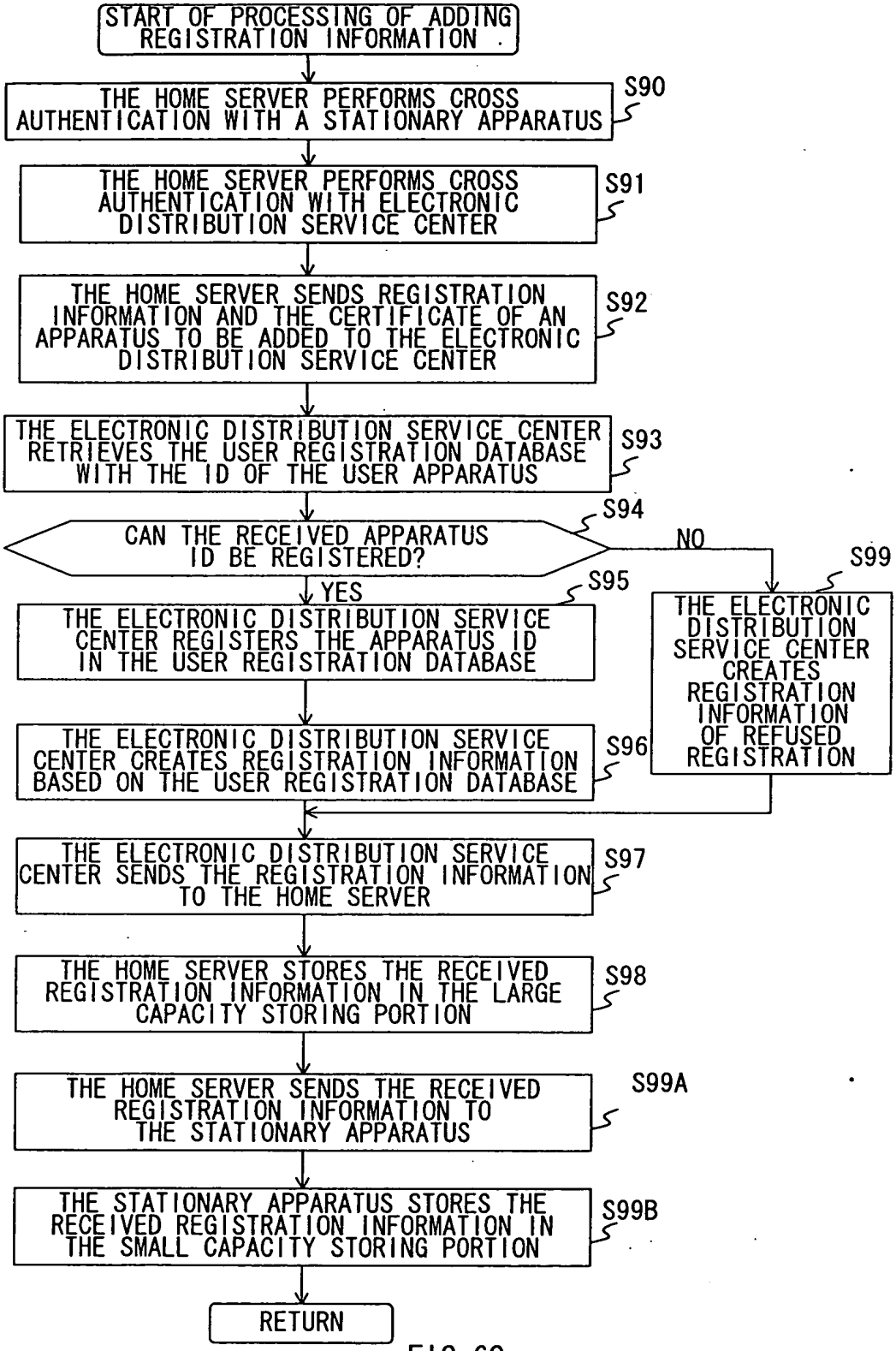
START OF PROCESSING OF ADDING REGISTRATION INFORMATION
THE HOME SERVER PERFORMS CROSS AUTHENTICATION WITH A STATIONARY APPARATUS
S90
THE HOME SERVER PERFORMS CROSS AUTHENTICATION WITH ELECTRONIC DISTRIBUTION SERVICE CENTER
S91
THE HOME SERVER SENDS REGISTRATION INFORMATION AND THE CERTIFICATE OF AN APPARATUS TO BE ADDED TO THE ELECTRONIC DISTRIBUTION SERVICE CENTER
S92
THE ELECTRONIC DISTRIBUTION SERVICE CENTER RETRIEVES THE USER REGISTRATION DATABASE WITH THE ID OF THE USER APPARATUS
S93
CAN THE RECEIVED APPARATUS ID BE REGISTERED?
S94
NO
YES
S99
THE ELECTRONIC DISTRIBUTION SERVICE CENTER CREATES REGISTRATION INFORMATION OF REFUSED REGISTRATION
S95
THE ELECTRONIC DISTRIBUTION SERVICE CENTER REGISTERS THE APPARATUS ID IN THE USER REGISTRATION DATABASE
THE ELECTRONIC DISTRIBUTION SERVICE CENTER CREATES REGISTRATION INFORMATION BASED ON THE USER REGISTRATION DATABASE
S96
THE ELECTRONIC DISTRIBUTION SERVICE CENTER SENDS THE REGISTRATION INFORMATION TO THE HOME SERVER
S97
THE HOME SERVER STORES THE RECEIVED REGISTRATION INFORMATION IN THE LARGE CAPACITY STORING PORTION
S98
THE HOME SERVER SENDS THE RECEIVED REGISTRATION INFORMATION TO THE STATIONARY APPARATUS
S99A
THE STATIONARY APPARATUS STORES THE RECEIVED REGISTRATION INFORMATION IN THE SMALL CAPACITY STORING PORTION
S99B
RETURN

FIG. 60

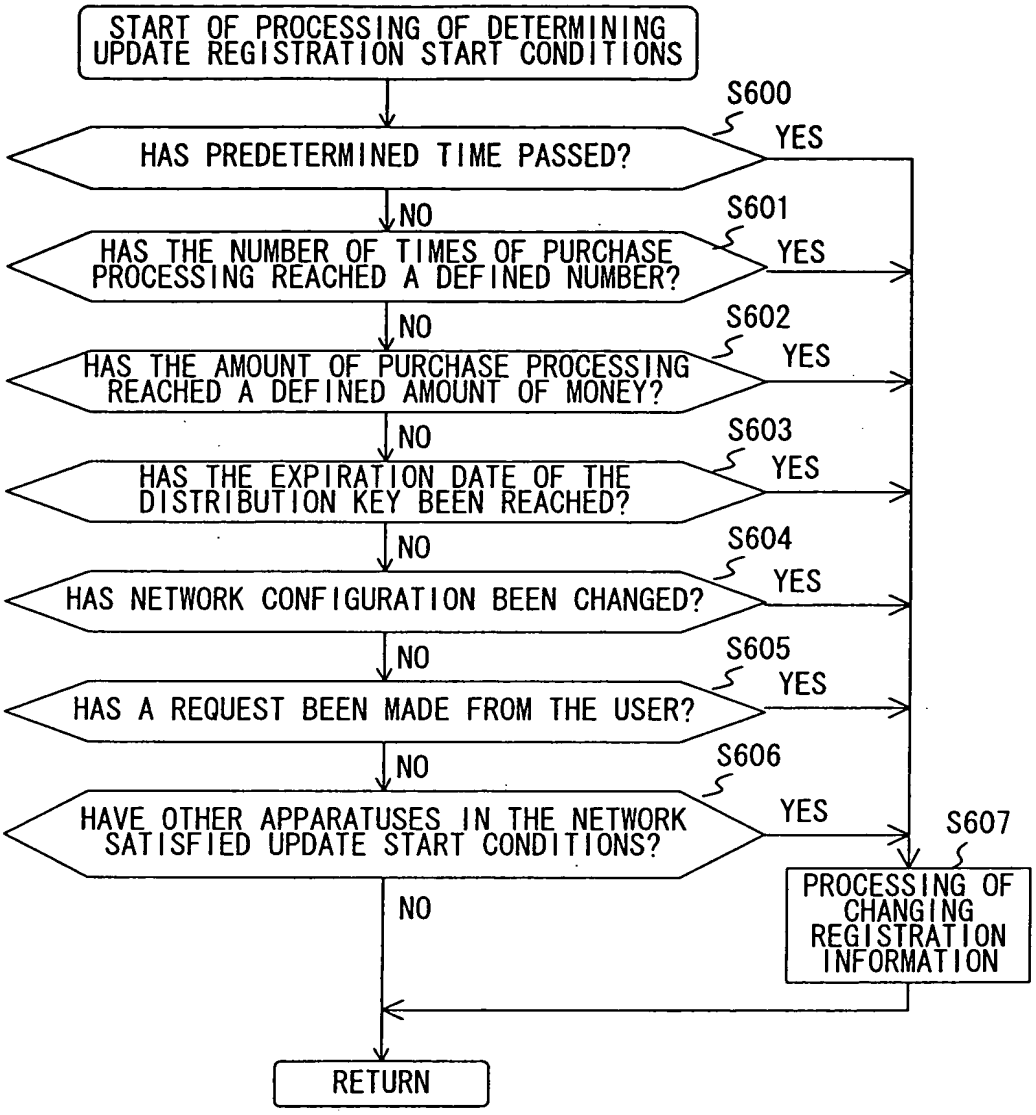
START OF PROCESSING OF DETERMINING UPDATE REGISTRATION START CONDITIONS
S600
HAS PREDETERMINED TIME PASSED?
YES
NO
S601
HAS THE NUMBER OF TIMES OF PURCHASE PROCESSING REACHED A DEFINED NUMBER?
YES
NO
S602
HAS THE AMOUNT OF PURCHASE PROCESSING REACHED A DEFINED AMOUNT OF MONEY?
YES
NO
S603
HAS THE EXPIRATION DATE OF THE DISTRIBUTION KEY BEEN REACHED?
YES
NO
S604
HAS NETWORK CONFIGURATION BEEN CHANGED?
YES
NO
S605
HAS A REQUEST BEEN MADE FROM THE USER?
YES
NO
S606
HAVE OTHER APPARATUSES IN THE NETWORK SATISFIED UPDATE START CONDITIONS?
YES
NO
S607
PROCESSING OF CHANGING REGISTRATION INFORMATION
RETURN

FIG. 61

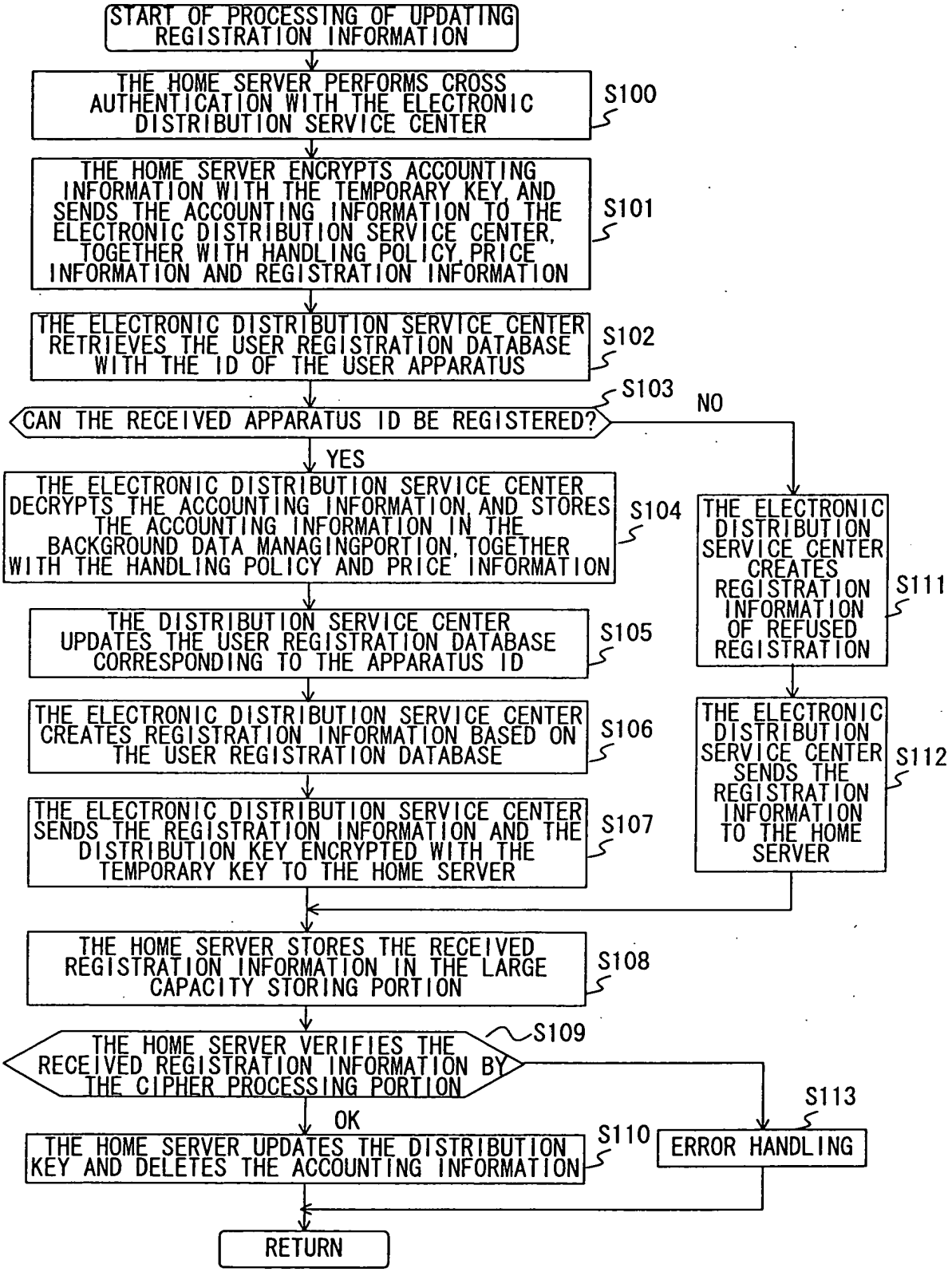
START OF PROCESSING OF UPDATING REGISTRATION INFORMATION
THE HOME SERVER PERFORMS CROSS AUTHENTICATION WITH THE ELECTRONIC DISTRIBUTION SERVICE CENTER
S100
THE HOME SERVER ENCRYPTS ACCOUNTING INFORMATION WITH THE TEMPORARY KEY, AND SENDS THE ACCOUNTING INFORMATION TO THE ELECTRONIC DISTRIBUTION SERVICE CENTER, TOGETHER WITH HANDLING POLICY, PRICE INFORMATION AND REGISTRATION INFORMATION
S101
THE ELECTRONIC DISTRIBUTION SERVICE CENTER RETRIEVES THE USER REGISTRATION DATABASE WITH THE ID OF THE USER APPARATUS
S102
S103
CAN THE RECEIVED APPARATUS ID BE REGISTERED?
NO
YES
THE ELECTRONIC DISTRIBUTION SERVICE CENTER DECRYPTS THE ACCOUNTING INFORMATION, AND STORES THE ACCOUNTING INFORMATION IN THE BACKGROUND DATA MANAGINGPORTION, TOGETHER WITH THE HANDLING POLICY AND PRICE INFORMATION
S104
THE ELECTRONIC DISTRIBUTION SERVICE CENTER CREATES REGISTRATION INFORMATION OF REFUSED REGISTRATION
S111
THE DISTRIBUTION SERVICE CENTER UPDATES THE USER REGISTRATION DATABASE CORRESPONDING TO THE APPARATUS ID
S105
THE ELECTRONIC DISTRIBUTION SERVICE CENTER CREATES REGISTRATION INFORMATION BASED ON THE USER REGISTRATION DATABASE
S106
THE ELECTRONIC DISTRIBUTION SERVICE CENTER SENDS THE REGISTRATION INFORMATION TO THE HOME SERVER
S112
THE ELECTRONIC DISTRIBUTION SERVICE CENTER SENDS THE REGISTRATION INFORMATION AND THE DISTRIBUTION KEY ENCRYPTED WITH THE TEMPORARY KEY TO THE HOME SERVER
S107
THE HOME SERVER STORES THE RECEIVED REGISTRATION INFORMATION IN THE LARGE CAPACITY STORING PORTION
S108
THE HOME SERVER VERIFIES THE RECEIVED REGISTRATION INFORMATION BY THE CIPHER PROCESSING PORTION
S109
S113
OK
THE HOME SERVER UPDATES THE DISTRIBUTION KEY AND DELETES THE ACCOUNTING INFORMATION
S110
ERROR HANDLING
RETURN

FIG. 62

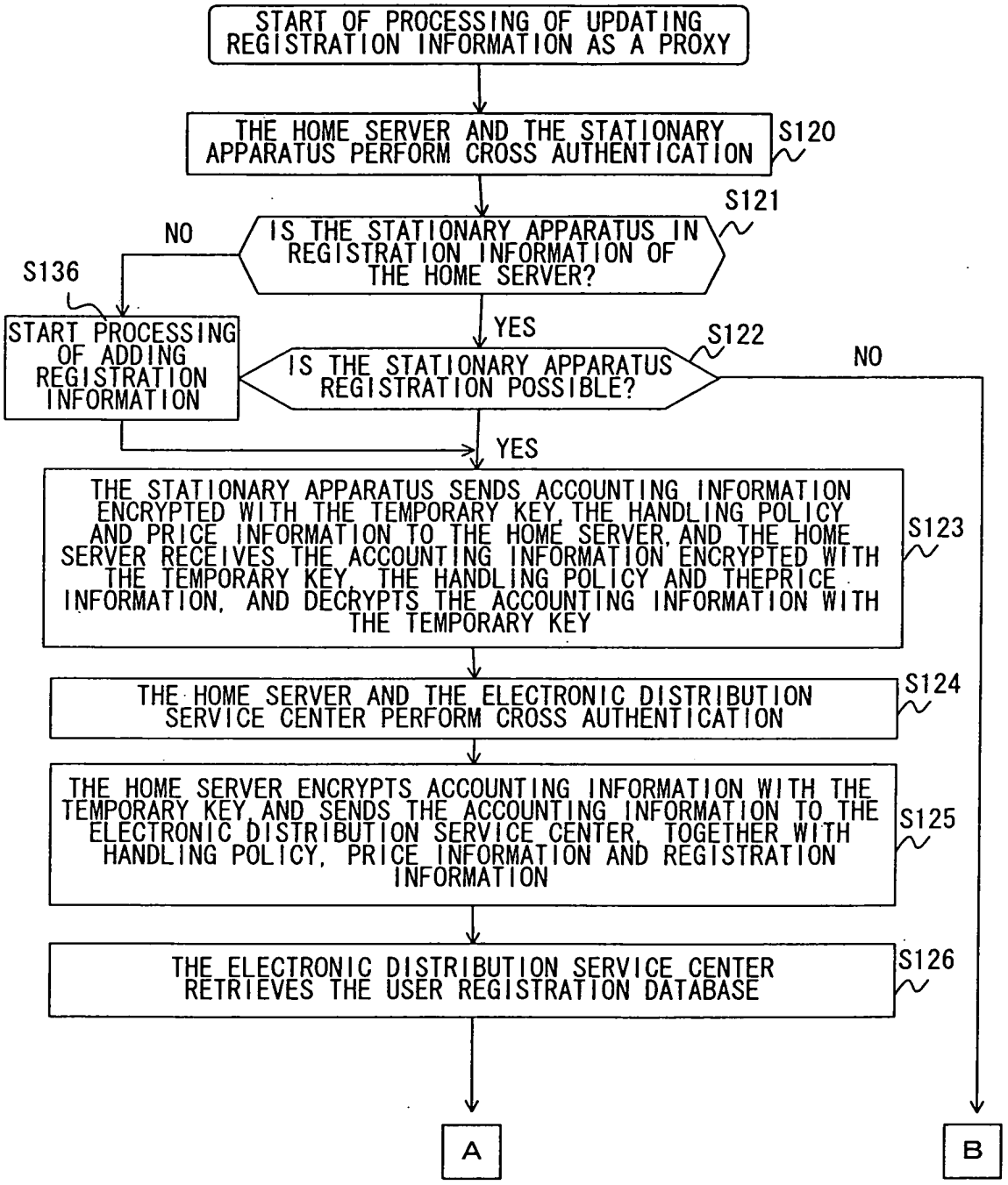

FIG. 63

09830392 "050401

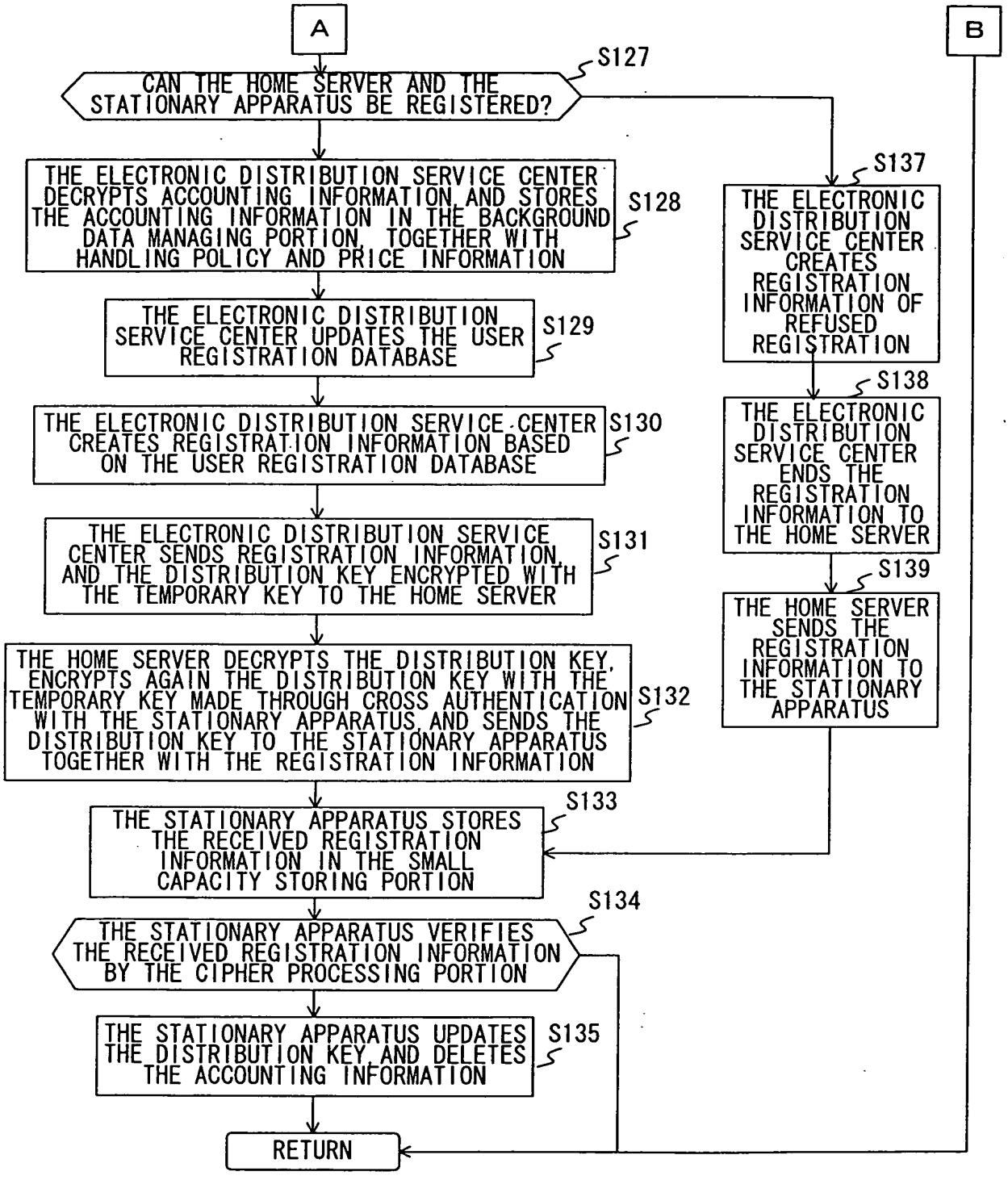

FIG. 64

09830392.060801

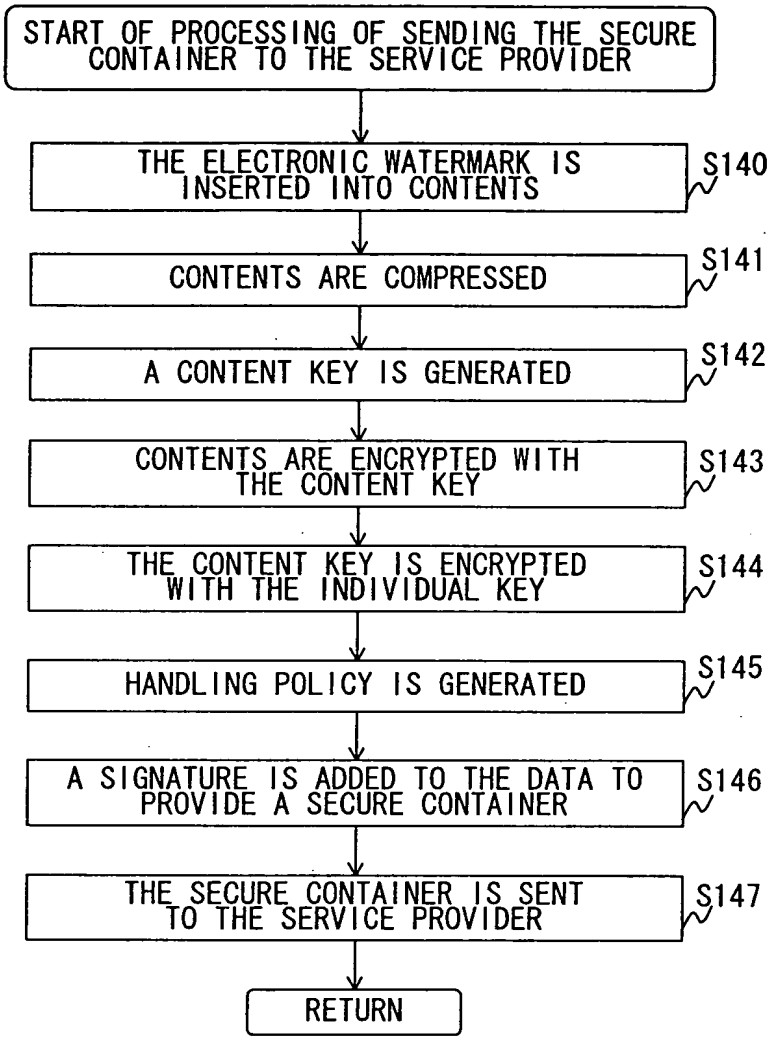
START OF PROCESSING OF SENDING THE SECURE CONTAINER TO THE SERVICE PROVIDER
THE ELECTRONIC WATERMARK IS INSERTED INTO CONTENTS
S140
CONTENTS ARE COMPRESSED
S141
A CONTENT KEY IS GENERATED
S142
CONTENTS ARE ENCRYPTED WITH THE CONTENT KEY
S143
THE CONTENT KEY IS ENCRYPTED WITH THE INDIVIDUAL KEY
S144
HANDLING POLICY IS GENERATED
S145
A SIGNATURE IS ADDED TO THE DATA TO PROVIDE A SECURE CONTAINER
S146
THE SECURE CONTAINER IS SENT TO THE SERVICE PROVIDER
S147
RETURN

FIG. 65

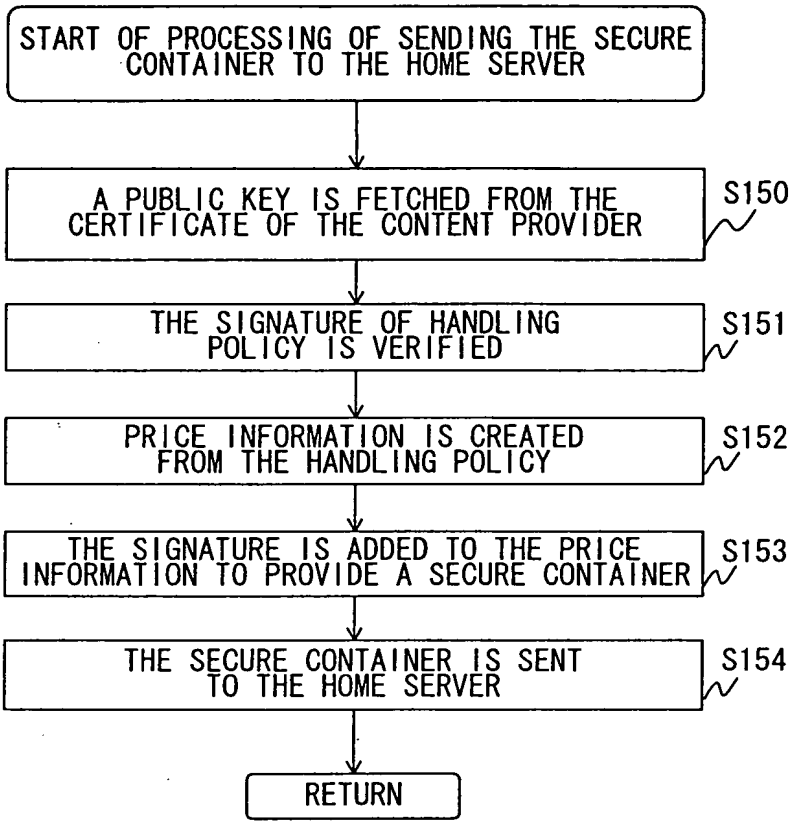
START OF PROCESSING OF SENDING THE SECURE CONTAINER TO THE HOME SERVER
A PUBLIC KEY IS FETCHED FROM THE CERTIFICATE OF THE CONTENT PROVIDER
S150
THE SIGNATURE OF HANDLING POLICY IS VERIFIED
S151
PRICE INFORMATION IS CREATED FROM THE HANDLING POLICY
S152
THE SIGNATURE IS ADDED TO THE PRICE INFORMATION TO PROVIDE A SECURE CONTAINER
S153
THE SECURE CONTAINER IS SENT TO THE HOME SERVER
S154
RETURN

FIG. 66

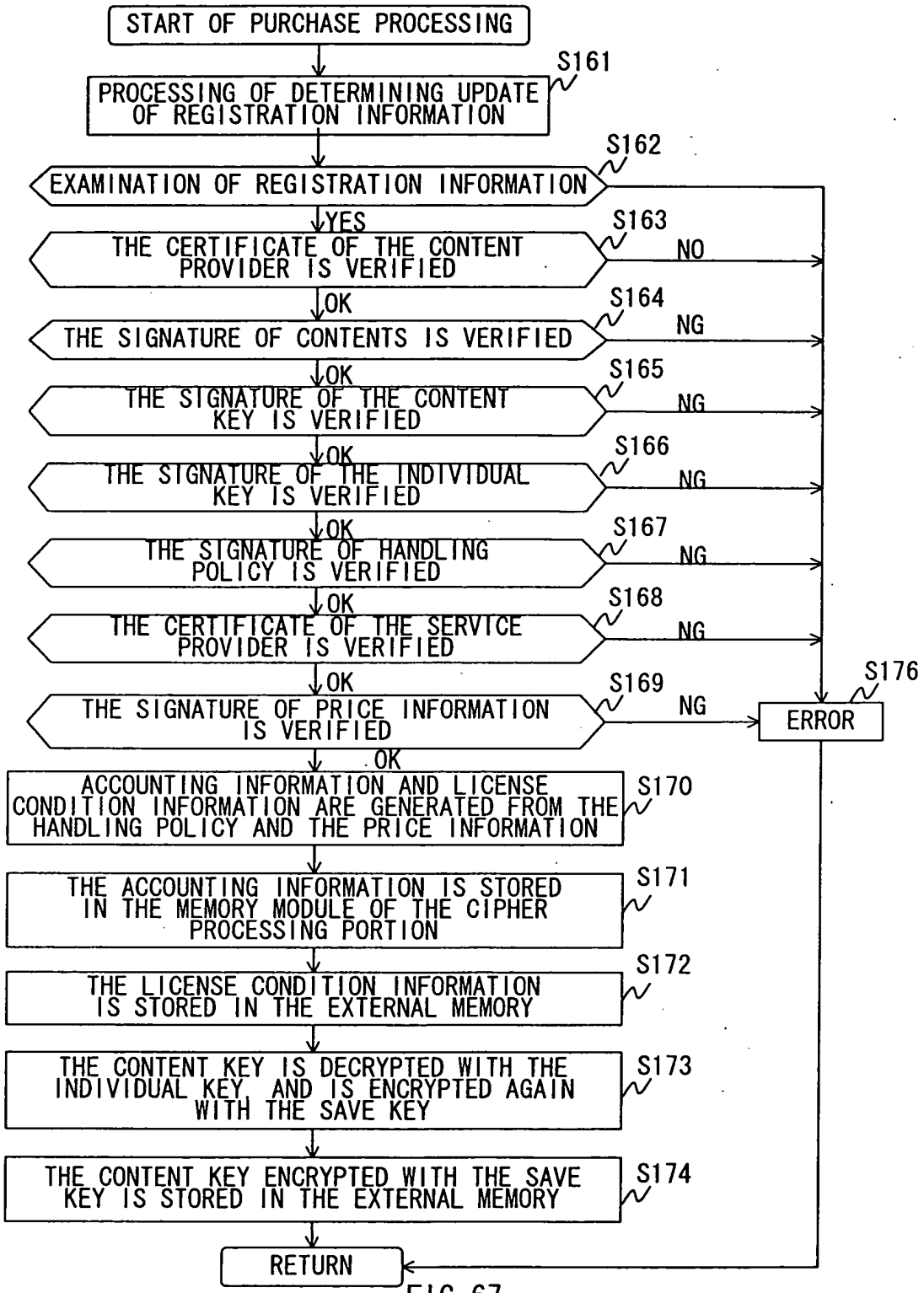
START OF PURCHASE PROCESSING
S161
PROCESSING OF DETERMINING UPDATE OF REGISTRATION INFORMATION
S162
EXAMINATION OF REGISTRATION INFORMATION
YES
S163
THE CERTIFICATE OF THE CONTENT PROVIDER IS VERIFIED
NO
OK
S164
THE SIGNATURE OF CONTENTS IS VERIFIED
NG
OK
S165
THE SIGNATURE OF THE CONTENT KEY IS VERIFIED
NG
OK
S166
THE SIGNATURE OF THE INDIVIDUAL KEY IS VERIFIED
NG
OK
S167
THE SIGNATURE OF HANDLING POLICY IS VERIFIED
NG
OK
S168
THE CERTIFICATE OF THE SERVICE PROVIDER IS VERIFIED
NG
OK
S169
THE SIGNATURE OF PRICE INFORMATION IS VERIFIED
NG
S176
ERROR
OK
S170
ACCOUNTING INFORMATION AND LICENSE CONDITION INFORMATION ARE GENERATED FROM THE HANDLING POLICY AND THE PRICE INFORMATION
S171
THE ACCOUNTING INFORMATION IS STORED IN THE MEMORY MODULE OF THE CIPHER PROCESSING PORTION
S172
THE LICENSE CONDITION INFORMATION IS STORED IN THE EXTERNAL MEMORY
S173
THE CONTENT KEY IS DECRYPTED WITH THE INDIVIDUAL KEY, AND IS ENCRYPTED AGAIN WITH THE SAVE KEY
S174
THE CONTENT KEY ENCRYPTED WITH THE SAVE KEY IS STORED IN THE EXTERNAL MEMORY
RETURN

FIG. 67

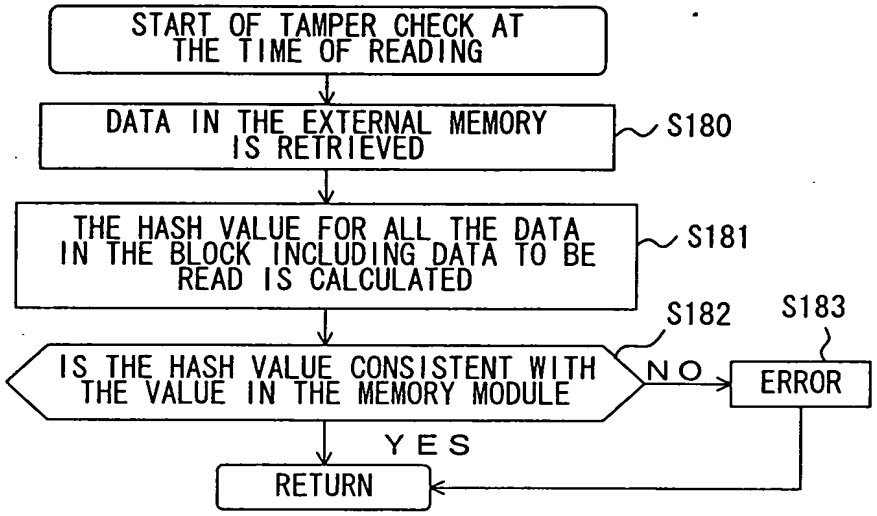
START OF TAMPER CHECK AT THE TIME OF READING
DATA IN THE EXTERNAL MEMORY IS RETRIEVED
S180
THE HASH VALUE FOR ALL THE DATA IN THE BLOCK INCLUDING DATA TO BE READ IS CALCULATED
S181
S182
S183
IS THE HASH VALUE CONSISTENT WITH THE VALUE IN THE MEMORY MODULE
NO
ERROR
YES
RETURN

FIG. 68

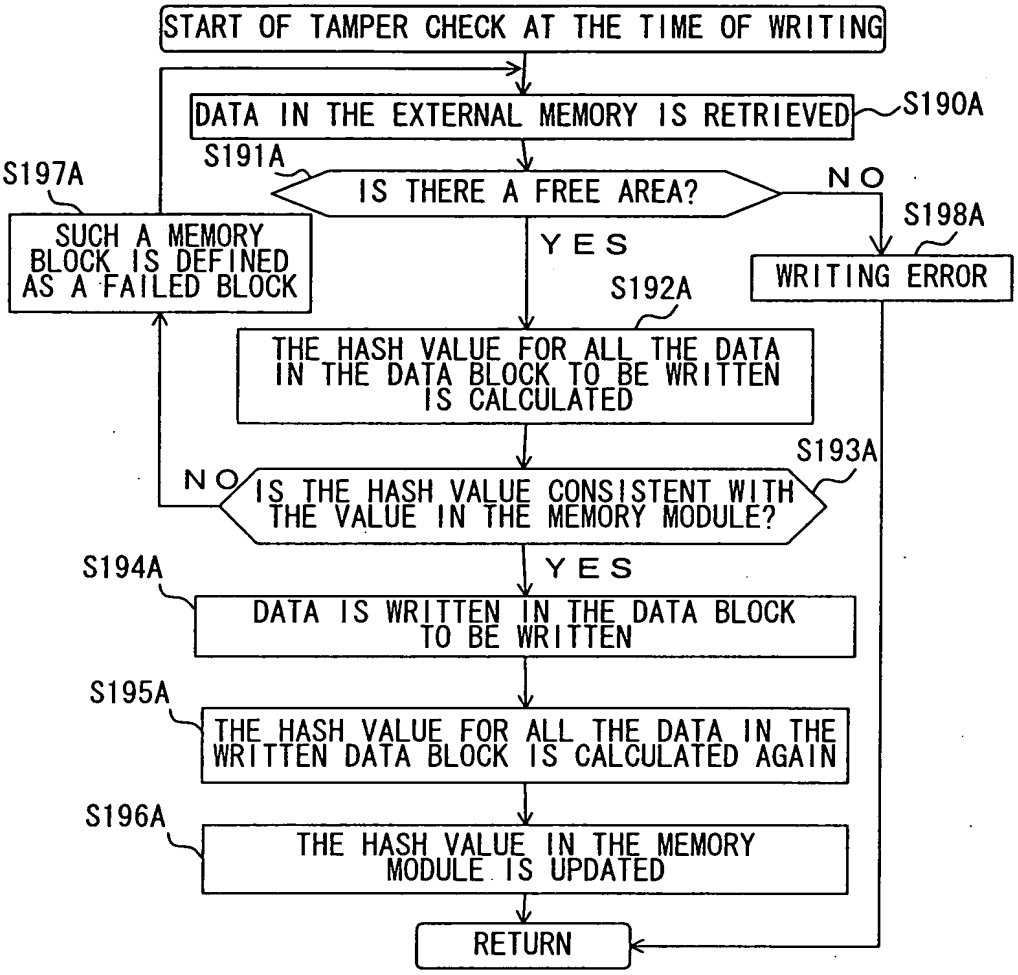
START OF TAMPER CHECK AT THE TIME OF WRITING
DATA IN THE EXTERNAL MEMORY IS RETRIEVED
S190A
S191A
IS THERE A FREE AREA?
NO
YES
S197A
SUCH A MEMORY BLOCK IS DEFINED AS A FAILED BLOCK
S198A
WRITING ERROR
S192A
THE HASH VALUE FOR ALL THE DATA IN THE DATA BLOCK TO BE WRITTEN IS CALCULATED
S193A
NO
IS THE HASH VALUE CONSISTENT WITH THE VALUE IN THE MEMORY MODULE?
YES
S194A
DATA IS WRITTEN IN THE DATA BLOCK TO BE WRITTEN
S195A
THE HASH VALUE FOR ALL THE DATA IN THE WRITTEN DATA BLOCK IS CALCULATED AGAIN
S196A
THE HASH VALUE IN THE MEMORY MODULE IS UPDATED
RETURN

FIG. 69

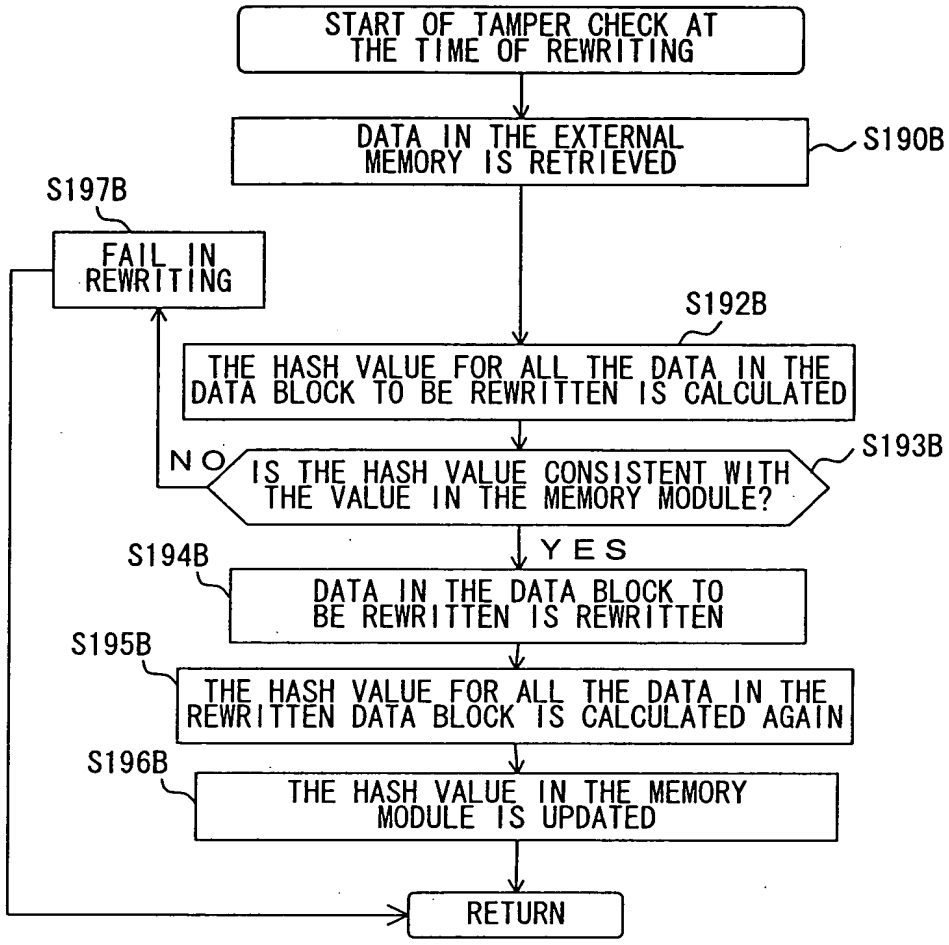
START OF TAMPER CHECK AT THE TIME OF REWRITING
DATA IN THE EXTERNAL MEMORY IS RETRIEVED
S190B
S197B
FAIL IN REWRITING
S192B
THE HASH VALUE FOR ALL THE DATA IN THE DATA BLOCK TO BE REWRITTEN IS CALCULATED
NO
IS THE HASH VALUE CONSISTENT WITH THE VALUE IN THE MEMORY MODULE?
S193B
YES
S194B
DATA IN THE DATA BLOCK TO BE REWRITTEN IS REWRITTEN
S195B
THE HASH VALUE FOR ALL THE DATA IN THE REWRITTEN DATA BLOCK IS CALCULATED AGAIN
S196B
THE HASH VALUE IN THE MEMORY MODULE IS UPDATED
RETURN

FIG. 70

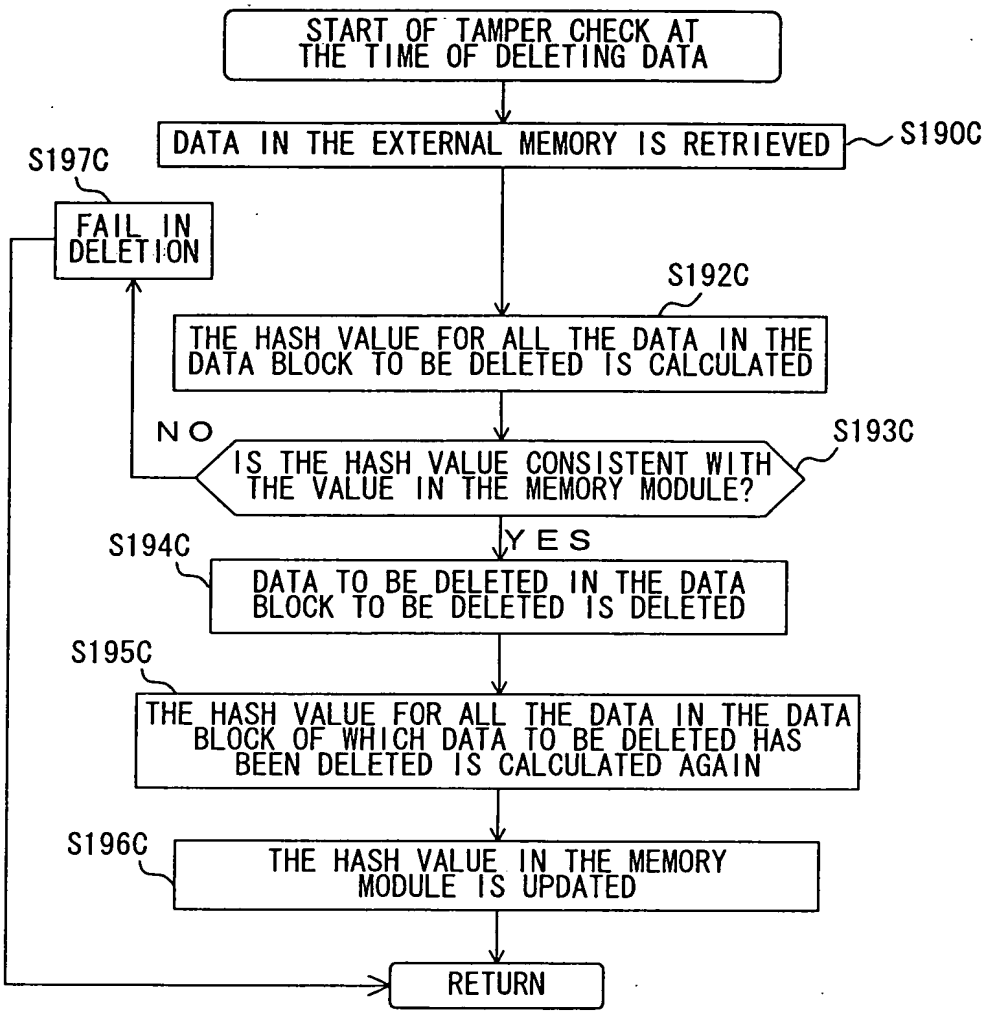
START OF TAMPER CHECK AT THE TIME OF DELETING DATA
DATA IN THE EXTERNAL MEMORY IS RETRIEVED
S190C
S197C
FAIL IN DELETION
S192C
THE HASH VALUE FOR ALL THE DATA IN THE DATA BLOCK TO BE DELETED IS CALCULATED
NO
IS THE HASH VALUE CONSISTENT WITH THE VALUE IN THE MEMORY MODULE?
S193C
YES
S194C
DATA TO BE DELETED IN THE DATA BLOCK TO BE DELETED IS DELETED
S195C
THE HASH VALUE FOR ALL THE DATA IN THE DATA BLOCK OF WHICH DATA TO BE DELETED HAS BEEN DELETED IS CALCULATED AGAIN
S196C
THE HASH VALUE IN THE MEMORY MODULE IS UPDATED
RETURN

FIG. 71

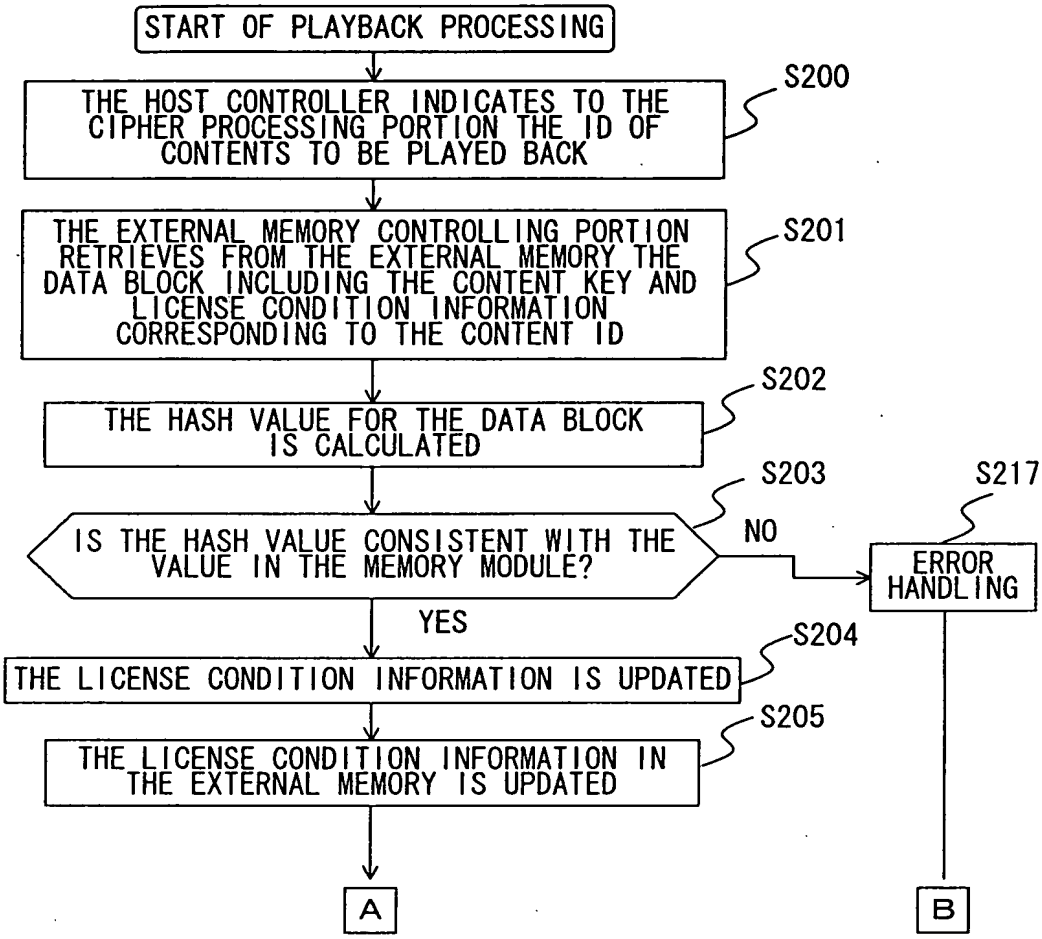
START OF PLAYBACK PROCESSING
THE HOST CONTROLLER INDICATES TO THE CIPHER PROCESSING PORTION THE ID OF CONTENTS TO BE PLAYED BACK
S200
THE EXTERNAL MEMORY CONTROLLING PORTION RETRIEVES FROM THE EXTERNAL MEMORY THE DATA BLOCK INCLUDING THE CONTENT KEY AND LICENSE CONDITION INFORMATION CORRESPONDING TO THE CONTENT ID
S201
THE HASH VALUE FOR THE DATA BLOCK IS CALCULATED
S202
IS THE HASH VALUE CONSISTENT WITH THE VALUE IN THE MEMORY MODULE?
S203
NO
ERROR HANDLING
S217
YES
THE LICENSE CONDITION INFORMATION IS UPDATED
S204
THE LICENSE CONDITION INFORMATION IN THE EXTERNAL MEMORY IS UPDATED
S205
A
B

FIG. 72

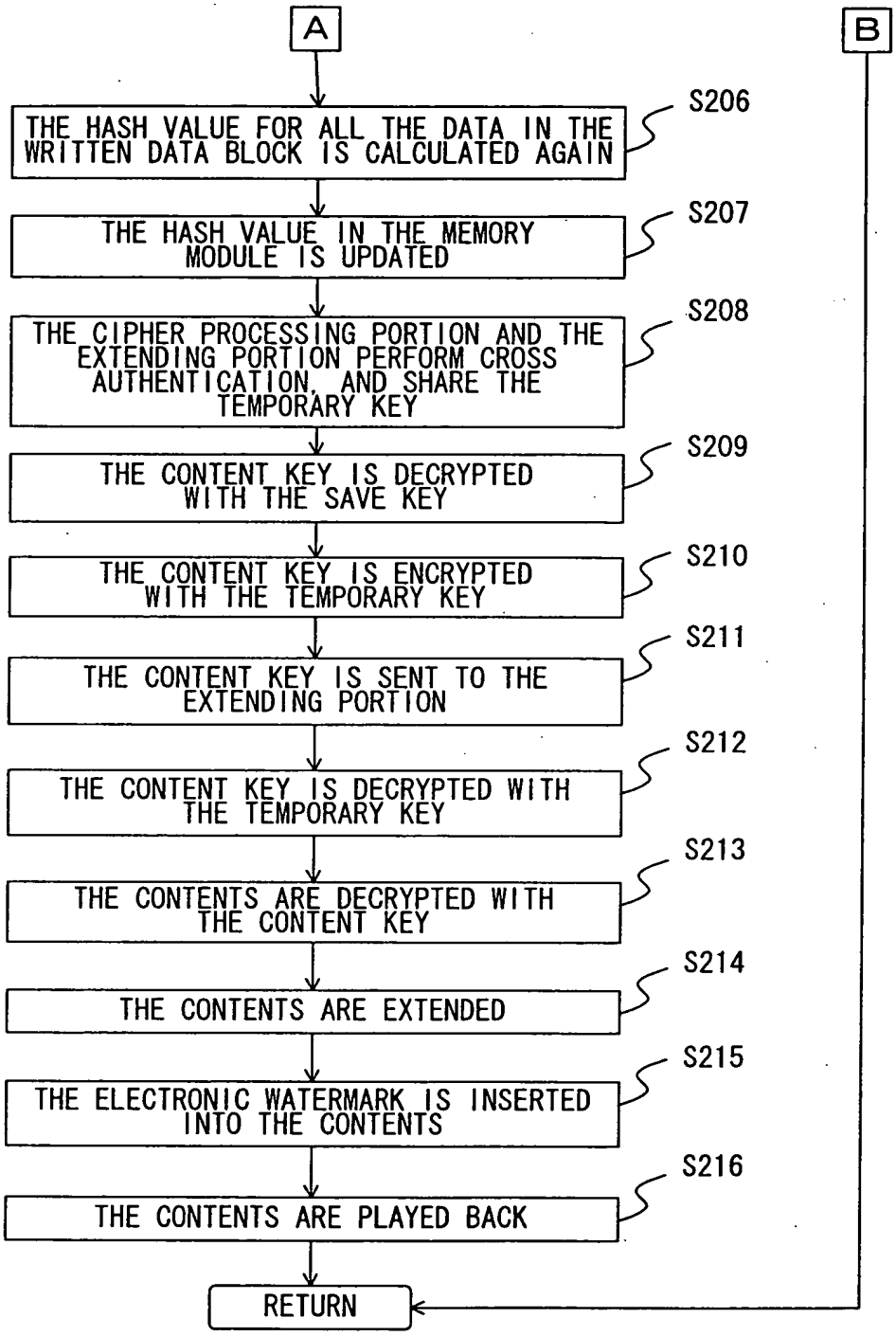
A
B
THE HASH VALUE FOR ALL THE DATA IN THE WRITTEN DATA BLOCK IS CALCULATED AGAIN
S206
THE HASH VALUE IN THE MEMORY MODULE IS UPDATED
S207
THE CIPHER PROCESSING PORTION AND THE EXTENDING PORTION PERFORM CROSS AUTHENTICATION, AND SHARE THE TEMPORARY KEY
S208
THE CONTENT KEY IS DECRYPTED WITH THE SAVE KEY
S209
THE CONTENT KEY IS ENCRYPTED WITH THE TEMPORARY KEY
S210
THE CONTENT KEY IS SENT TO THE EXTENDING PORTION
S211
THE CONTENT KEY IS DECRYPTED WITH THE TEMPORARY KEY
S212
THE CONTENTS ARE DECRYPTED WITH THE CONTENT KEY
S213
THE CONTENTS ARE EXTENDED
S214
THE ELECTRONIC WATERMARK IS INSERTED INTO THE CONTENTS
S215
THE CONTENTS ARE PLAYED BACK
S216
RETURN

FIG. 73

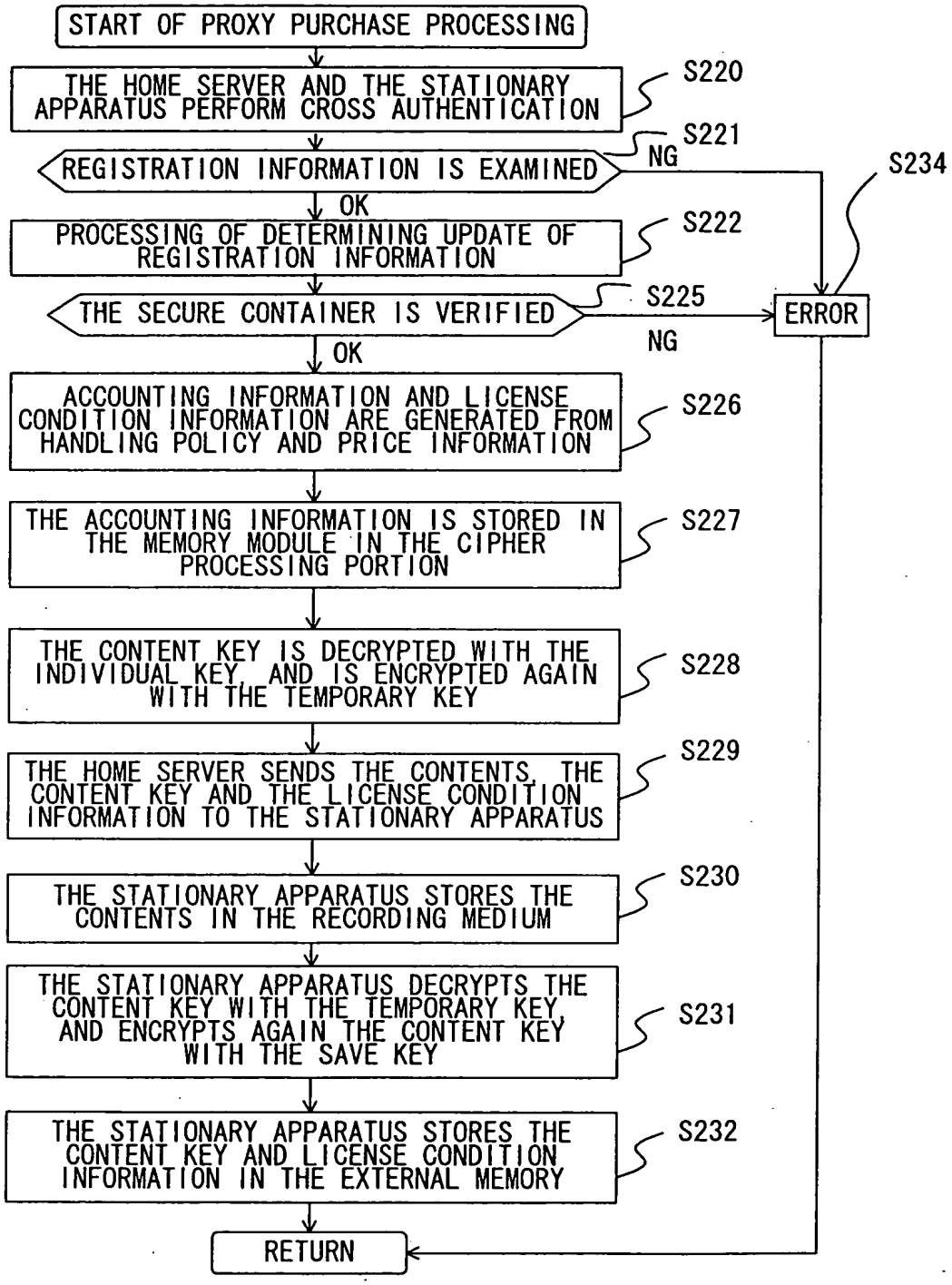

FIG. 74

09830392*050601

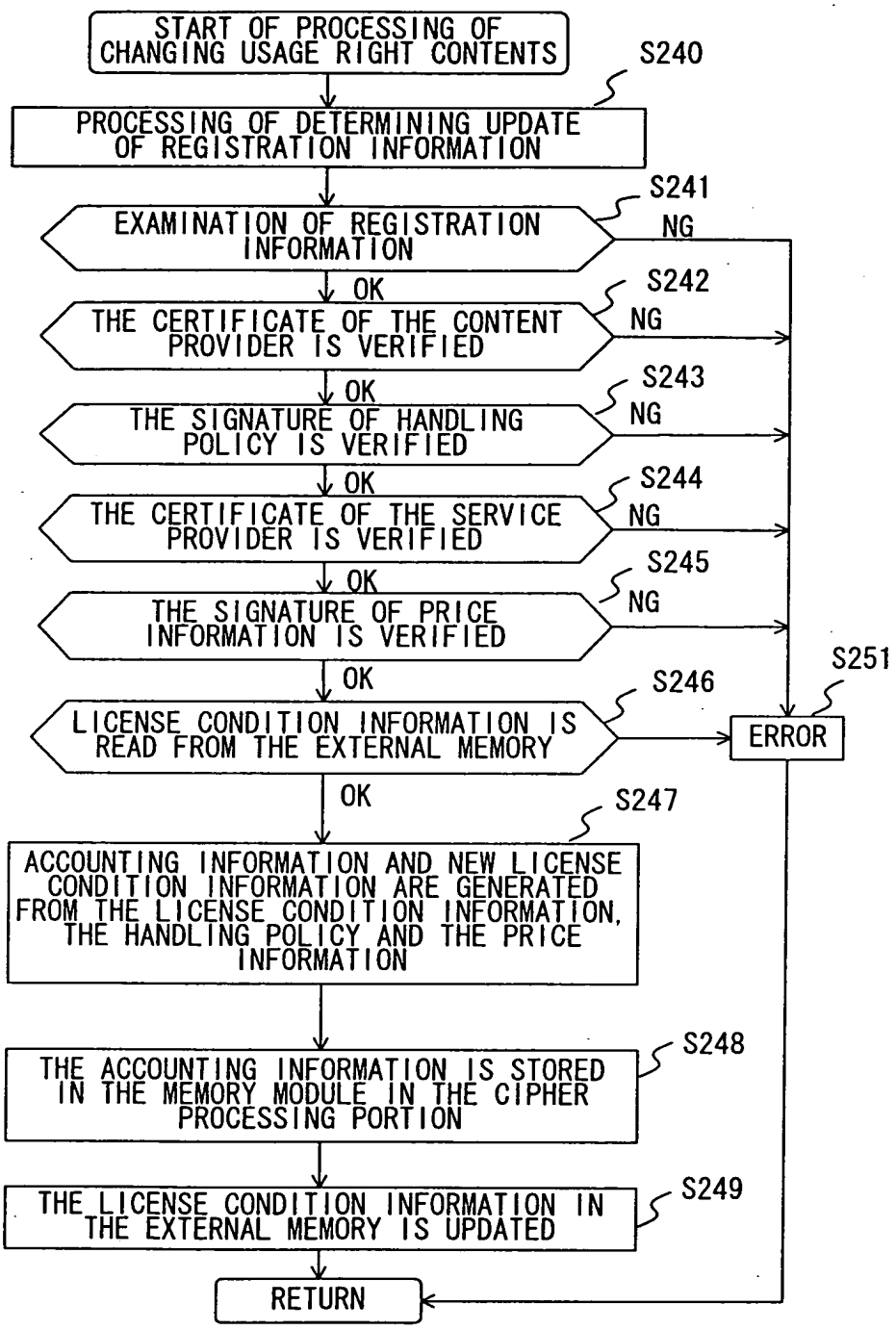
START OF PROCESSING OF CHANGING USAGE RIGHT CONTENTS
S240
PROCESSING OF DETERMINING UPDATE OF REGISTRATION INFORMATION
S241
EXAMINATION OF REGISTRATION INFORMATION
NG
OK
S242
THE CERTIFICATE OF THE CONTENT PROVIDER IS VERIFIED
NG
OK
S243
THE SIGNATURE OF HANDLING POLICY IS VERIFIED
NG
OK
S244
THE CERTIFICATE OF THE SERVICE PROVIDER IS VERIFIED
NG
OK
S245
THE SIGNATURE OF PRICE INFORMATION IS VERIFIED
NG
OK
S246
LICENSE CONDITION INFORMATION IS READ FROM THE EXTERNAL MEMORY
S251
ERROR
OK
S247
ACCOUNTING INFORMATION AND NEW LICENSE CONDITION INFORMATION ARE GENERATED FROM THE LICENSE CONDITION INFORMATION, THE HANDLING POLICY AND THE PRICE INFORMATION
S248
THE ACCOUNTING INFORMATION IS STORED IN THE MEMORY MODULE IN THE CIPHER PROCESSING PORTION
S249
THE LICENSE CONDITION INFORMATION IN THE EXTERNAL MEMORY IS UPDATED
RETURN

FIG. 75

RULE N	RULE NUMBER
	USAGE CONTENT RIGHT NUMBER
	PARAMETER
	MINIMUM PRICE
	EARNINGS (RATE OF BENEFITS)
RULE 1	RULE NUMBER #1
	USAGE RIGHT CONTENT NUMBER #1
	ABSENT
	￥３５０
	３０%
RULE 2	RULE NUMBER #2
	USAGE RIGHT CONTENT NUMBER #2
	ONE HOUR
	￥１００
	３０%
RULE 3	RULE NUMBER #3
	USAGE RIGHT CONTENT NUMBER #6
	ONE TIME
	￥３０
	３０%
RULE 4	RULE NUMBER #4
	USAGE RIGHT CONTENT NUMBER #13
	＃２／＃１
	￥２００
	２０%
RULE 5	RULE NUMBER #5
	USAGE RIGHT CONTENT NUMBER #14
	＃１／＃１
	￥２５０
	２０%

FIG. 76

RULE N	RULE NUMBER
	PARAMETER
	PRICE
RULE 1	RULE NUMBER #1
	３０%
	￥５００
RULE 2	RULE NUMBER #2
	４０%
	￥１００
RULE 3	RULE NUMBER #3
	４０%
	￥１００
RULE 4	RULE NUMBER #4
	１０%
	￥２００
RULE 5	RULE NUMBER #5
	２０%
	￥３５０

FIG. 77

09830392 - 051601

RULE 1	＃１
	＃１
	ABSENT
	￥３５０
	３０％
RULE 2	＃２
	＃２
	ONE HOUR
	￥１００
	３０％
RULE 3	＃３
	＃１３
	＃２／＃１
	￥２００
	２０％

ONE PART OF RULE PART
OF HANDLING POLICY

RULE 1	＃１
	３０％
	￥５００
RULE 2	＃２
	４０％
	￥１００
RULE 3	＃３
	１０％
	￥２００

ONE PART OF RULE PART
OF PRICE INFORMATION

PRESENT

RULE	RULE NUMBER
	USAGE RIGHT CONTENT NUMBER
	PARAMETER
RULE	＃２
	＃２
	THIRTY MINUTES / TWO HOURS

RULE PART OF LICENSE
CONDITION INFORMATION

AFTER CHANGE

RULE	RULE NUMBER
	USAGE RIGHT CONTENT NUMBER
	PARAMETER
RULE	＃１
	＃１
	ABSENT

RULE PART OF LICENSE
CONDITION INFORMATION

FIG. 78

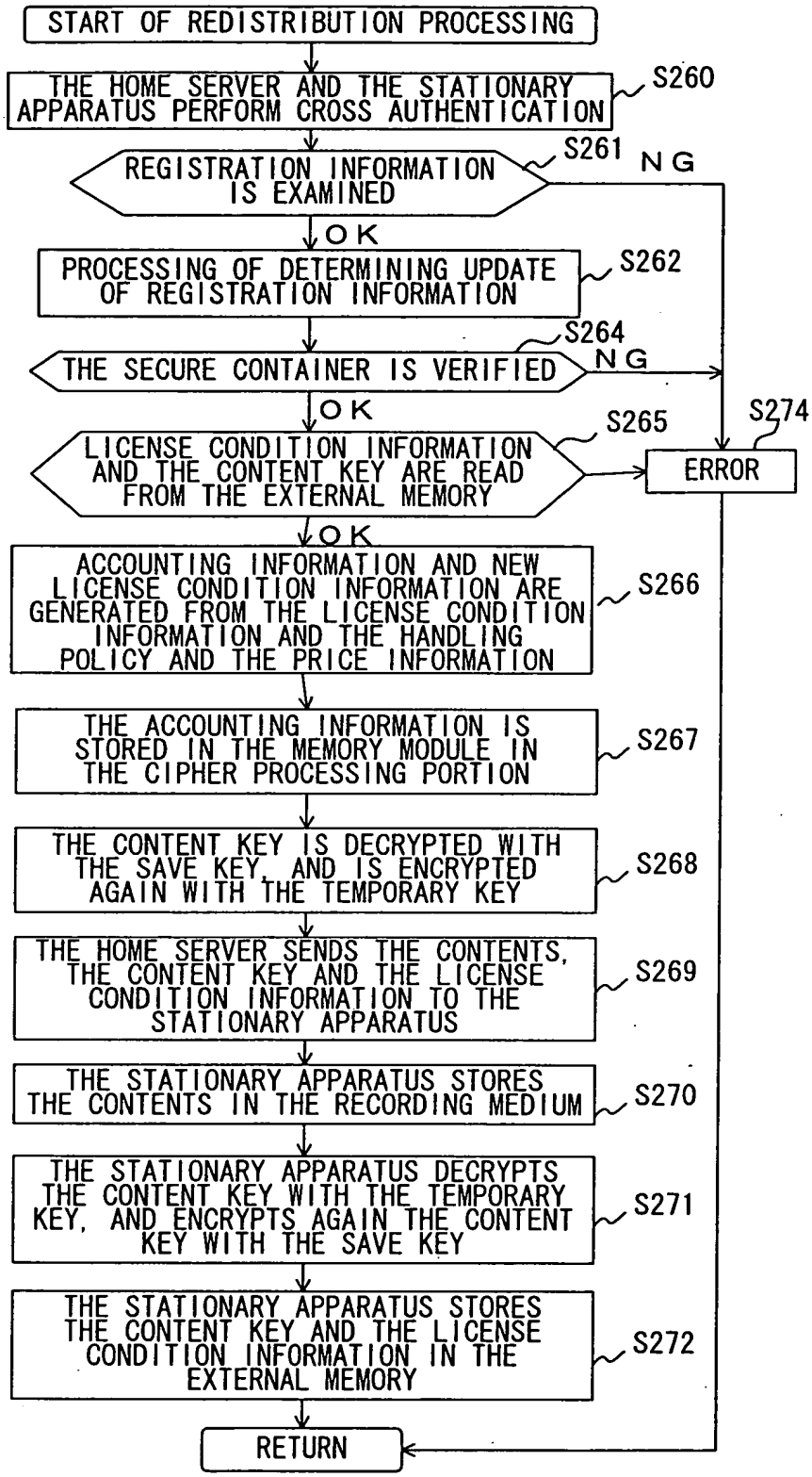
START OF REDISTRIBUTION PROCESSING
THE HOME SERVER AND THE STATIONARY APPARATUS PERFORM CROSS AUTHENTICATION
S260
REGISTRATION INFORMATION IS EXAMINED
S261
NG
OK
PROCESSING OF DETERMINING UPDATE OF REGISTRATION INFORMATION
S262
THE SECURE CONTAINER IS VERIFIED
S264
NG
OK
LICENSE CONDITION INFORMATION AND THE CONTENT KEY ARE READ FROM THE EXTERNAL MEMORY
S265
ERROR
S274
OK
ACCOUNTING INFORMATION AND NEW LICENSE CONDITION INFORMATION ARE GENERATED FROM THE LICENSE CONDITION INFORMATION AND THE HANDLING POLICY AND THE PRICE INFORMATION
S266
THE ACCOUNTING INFORMATION IS STORED IN THE MEMORY MODULE IN THE CIPHER PROCESSING PORTION
S267
THE CONTENT KEY IS DECRYPTED WITH THE SAVE KEY, AND IS ENCRYPTED AGAIN WITH THE TEMPORARY KEY
S268
THE HOME SERVER SENDS THE CONTENTS, THE CONTENT KEY AND THE LICENSE CONDITION INFORMATION TO THE STATIONARY APPARATUS
S269
THE STATIONARY APPARATUS STORES THE CONTENTS IN THE RECORDING MEDIUM
S270
THE STATIONARY APPARATUS DECRYPTS THE CONTENT KEY WITH THE TEMPORARY KEY, AND ENCRYPTS AGAIN THE CONTENT KEY WITH THE SAVE KEY
S271
THE STATIONARY APPARATUS STORES THE CONTENT KEY AND THE LICENSE CONDITION INFORMATION IN THE EXTERNAL MEMORY
S272
RETURN

FIG. 79

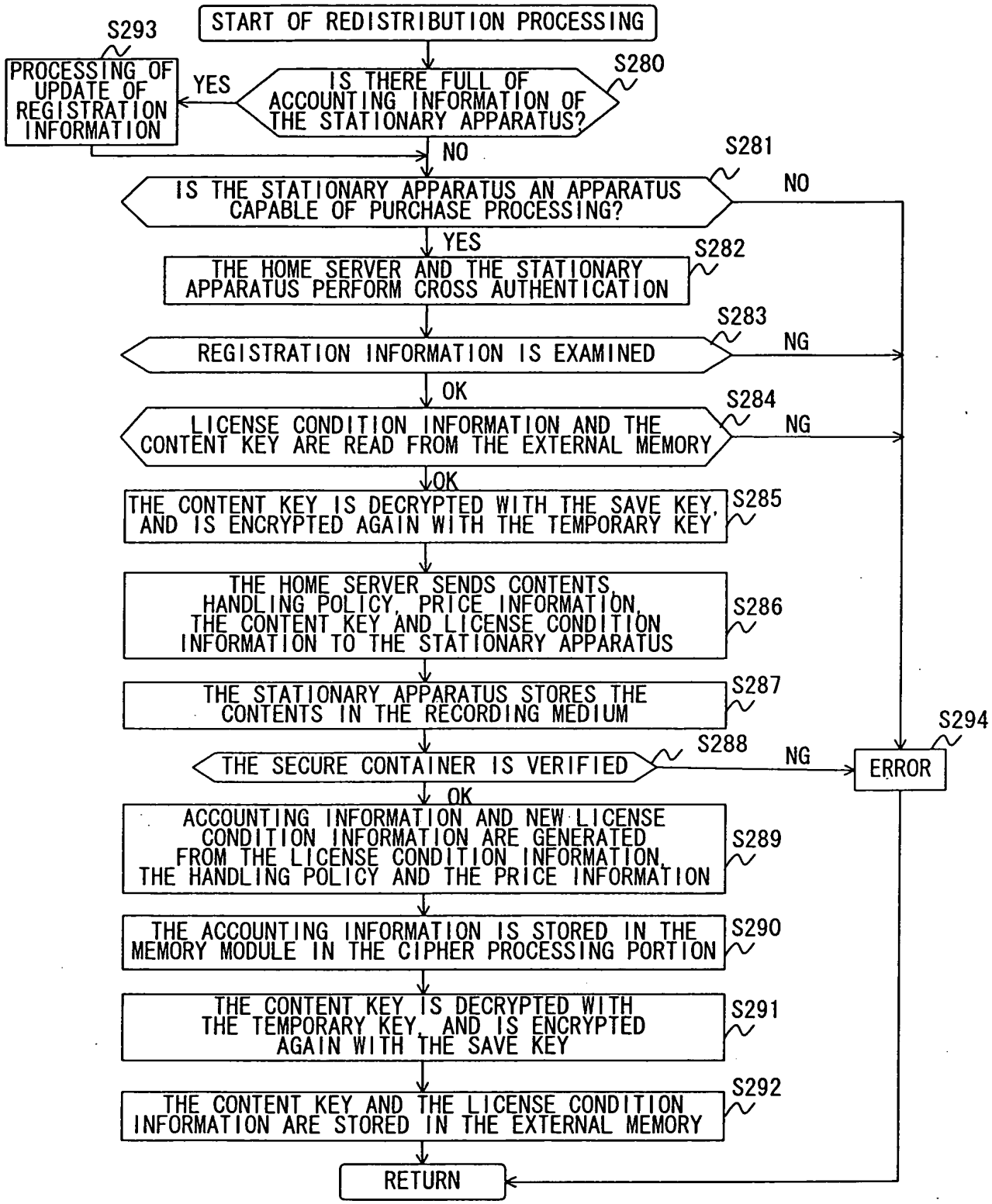

FIG. 80

FOR OFFICIAL USE ONLY

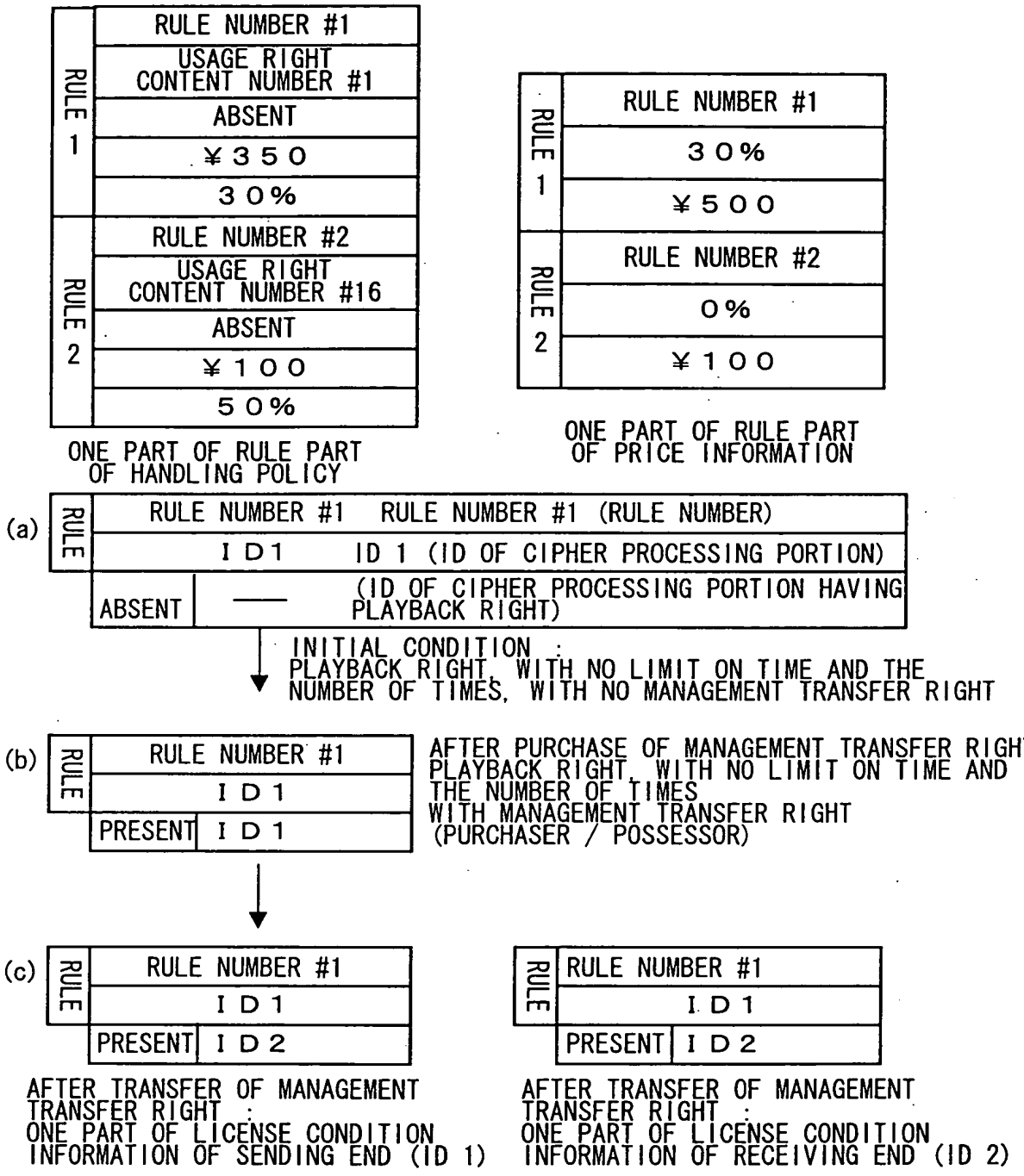
RULE 1
RULE NUMBER #1
USAGE RIGHT CONTENT NUMBER #1
ABSENT
¥350
30%
RULE 2
RULE NUMBER #2
USAGE RIGHT CONTENT NUMBER #16
ABSENT
¥100
50%
ONE PART OF RULE PART OF HANDLING POLICY
RULE 1
RULE NUMBER #1
30%
¥500
RULE 2
RULE NUMBER #2
0%
¥100
ONE PART OF RULE PART OF PRICE INFORMATION
(a)
RULE
RULE NUMBER #1 RULE NUMBER #1 (RULE NUMBER)
ID1 ID 1 (ID OF CIPHER PROCESSING PORTION)
ABSENT —— (ID OF CIPHER PROCESSING PORTION HAVING PLAYBACK RIGHT)
INITIAL CONDITION : PLAYBACK RIGHT, WITH NO LIMIT ON TIME AND THE NUMBER OF TIMES, WITH NO MANAGEMENT TRANSFER RIGHT
(b)
RULE
RULE NUMBER #1
ID1
PRESENT ID1
AFTER PURCHASE OF MANAGEMENT TRANSFER RIGHT : PLAYBACK RIGHT, WITH NO LIMIT ON TIME AND THE NUMBER OF TIMES WITH MANAGEMENT TRANSFER RIGHT (PURCHASER / POSSESSOR)
(c)
RULE
RULE NUMBER #1
ID1
PRESENT ID2
AFTER TRANSFER OF MANAGEMENT TRANSFER RIGHT : ONE PART OF LICENSE CONDITION INFORMATION OF SENDING END (ID 1)
RULE
RULE NUMBER #1
ID1
PRESENT ID2
AFTER TRANSFER OF MANAGEMENT TRANSFER RIGHT : ONE PART OF LICENSE CONDITION INFORMATION OF RECEIVING END (ID 2)

FIG. 81

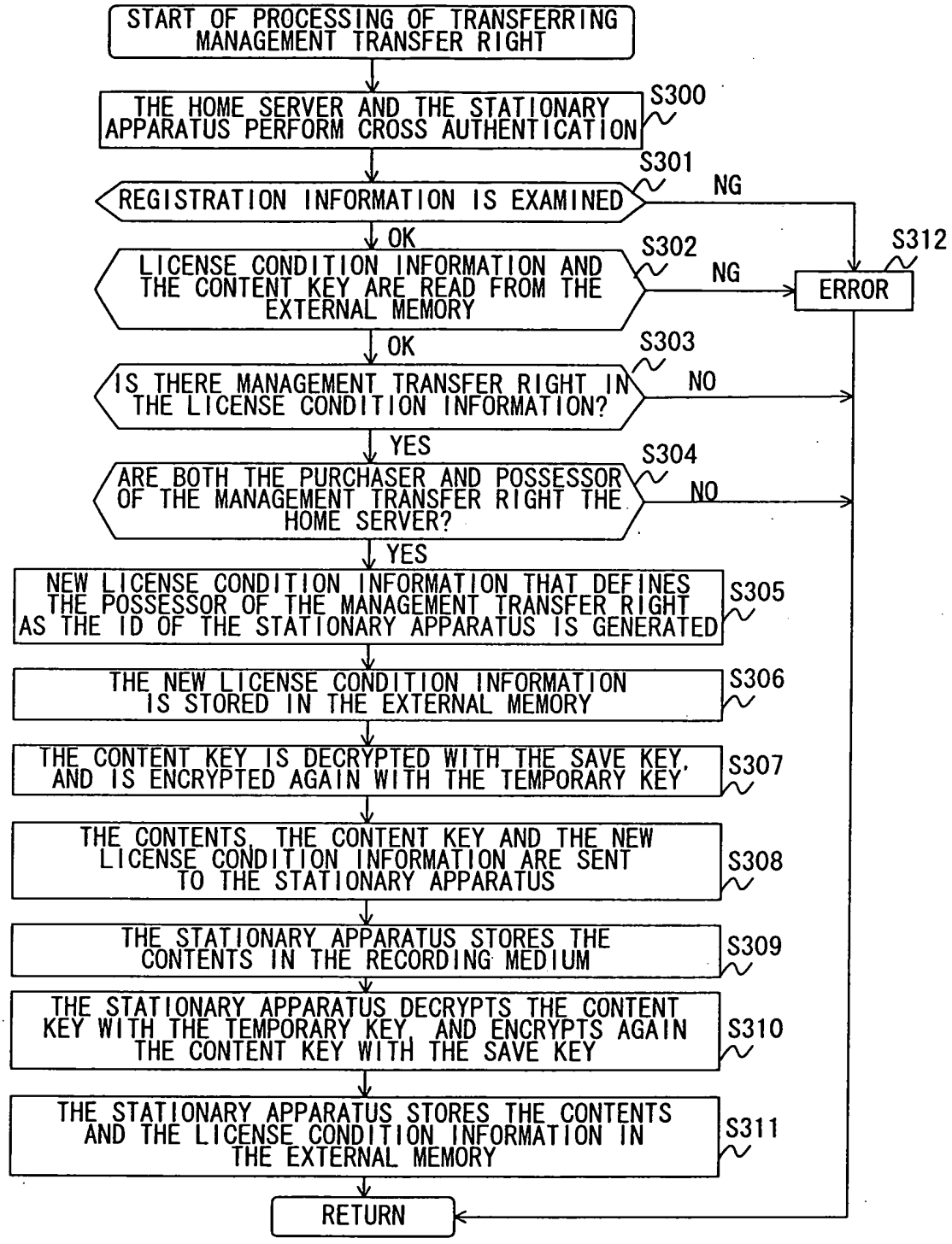
START OF PROCESSING OF TRANSFERRING MANAGEMENT TRANSFER RIGHT
THE HOME SERVER AND THE STATIONARY APPARATUS PERFORM CROSS AUTHENTICATION
S300
REGISTRATION INFORMATION IS EXAMINED
S301
NG
OK
LICENSE CONDITION INFORMATION AND THE CONTENT KEY ARE READ FROM THE EXTERNAL MEMORY
S302
NG
S312
ERROR
OK
IS THERE MANAGEMENT TRANSFER RIGHT IN THE LICENSE CONDITION INFORMATION?
S303
NO
YES
ARE BOTH THE PURCHASER AND POSSESSOR OF THE MANAGEMENT TRANSFER RIGHT THE HOME SERVER?
S304
NO
YES
NEW LICENSE CONDITION INFORMATION THAT DEFINES THE POSSESSOR OF THE MANAGEMENT TRANSFER RIGHT AS THE ID OF THE STATIONARY APPARATUS IS GENERATED
S305
THE NEW LICENSE CONDITION INFORMATION IS STORED IN THE EXTERNAL MEMORY
S306
THE CONTENT KEY IS DECRYPTED WITH THE SAVE KEY, AND IS ENCRYPTED AGAIN WITH THE TEMPORARY KEY
S307
THE CONTENTS, THE CONTENT KEY AND THE NEW LICENSE CONDITION INFORMATION ARE SENT TO THE STATIONARY APPARATUS
S308
THE STATIONARY APPARATUS STORES THE CONTENTS IN THE RECORDING MEDIUM
S309
THE STATIONARY APPARATUS DECRYPTS THE CONTENT KEY WITH THE TEMPORARY KEY, AND ENCRYPTS AGAIN THE CONTENT KEY WITH THE SAVE KEY
S310
THE STATIONARY APPARATUS STORES THE CONTENTS AND THE LICENSE CONDITION INFORMATION IN THE EXTERNAL MEMORY
S311
RETURN

FIG. 82

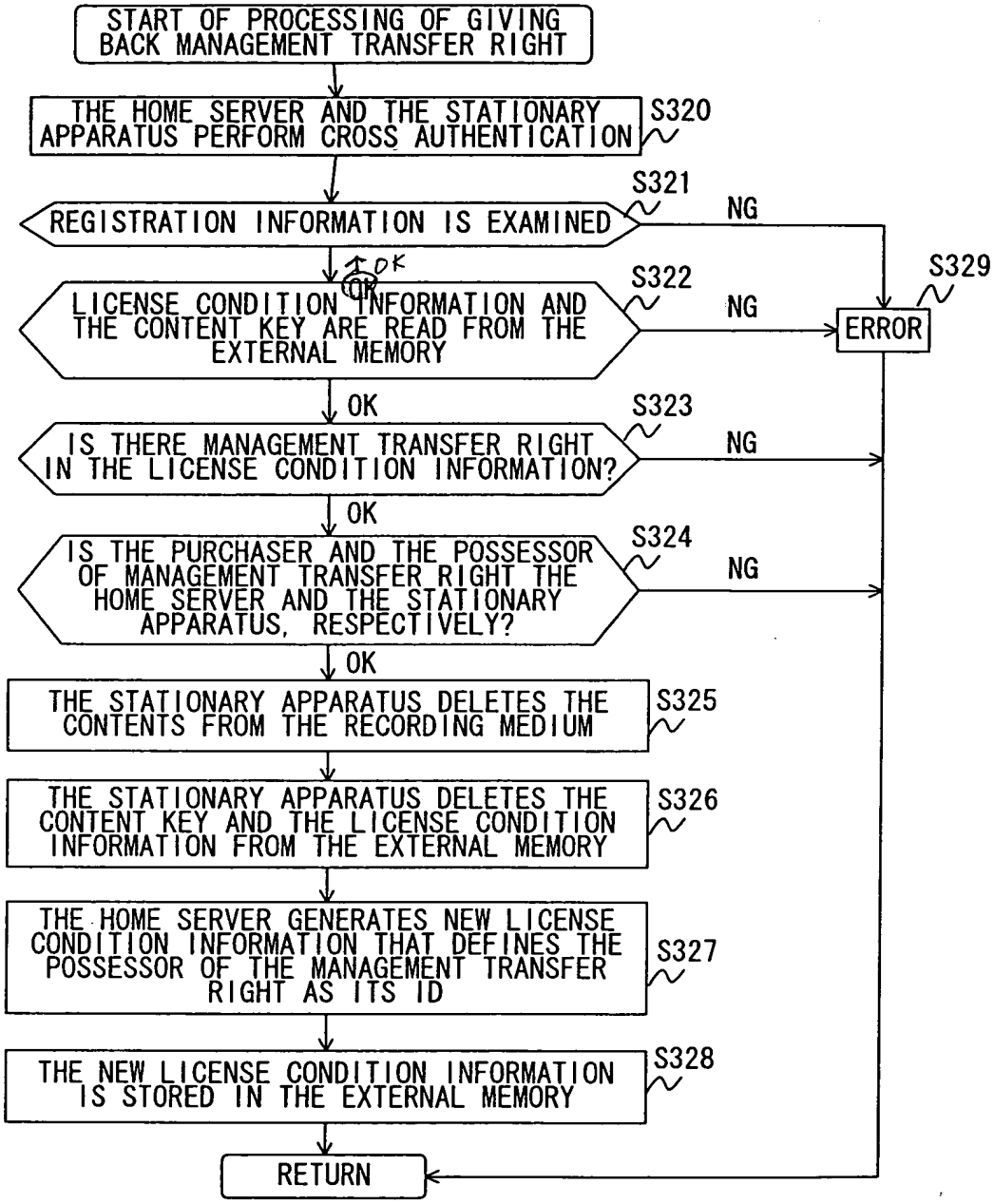
START OF PROCESSING OF GIVING BACK MANAGEMENT TRANSFER RIGHT
THE HOME SERVER AND THE STATIONARY APPARATUS PERFORM CROSS AUTHENTICATION
S320
REGISTRATION INFORMATION IS EXAMINED
S321
NG
OK
OR
LICENSE CONDITION INFORMATION AND THE CONTENT KEY ARE READ FROM THE EXTERNAL MEMORY
S322
NG
S329
ERROR
OK
IS THERE MANAGEMENT TRANSFER RIGHT IN THE LICENSE CONDITION INFORMATION?
S323
NG
OK
IS THE PURCHASER AND THE POSSESSOR OF MANAGEMENT TRANSFER RIGHT THE HOME SERVER AND THE STATIONARY APPARATUS, RESPECTIVELY?
S324
NG
OK
THE STATIONARY APPARATUS DELETES THE CONTENTS FROM THE RECORDING MEDIUM
S325
THE STATIONARY APPARATUS DELETES THE CONTENT KEY AND THE LICENSE CONDITION INFORMATION FROM THE EXTERNAL MEMORY
S326
THE HOME SERVER GENERATES NEW LICENSE CONDITION INFORMATION THAT DEFINES THE POSSESSOR OF THE MANAGEMENT TRANSFER RIGHT AS ITS ID
S327
THE NEW LICENSE CONDITION INFORMATION IS STORED IN THE EXTERNAL MEMORY
S328
RETURN

FIG. 83

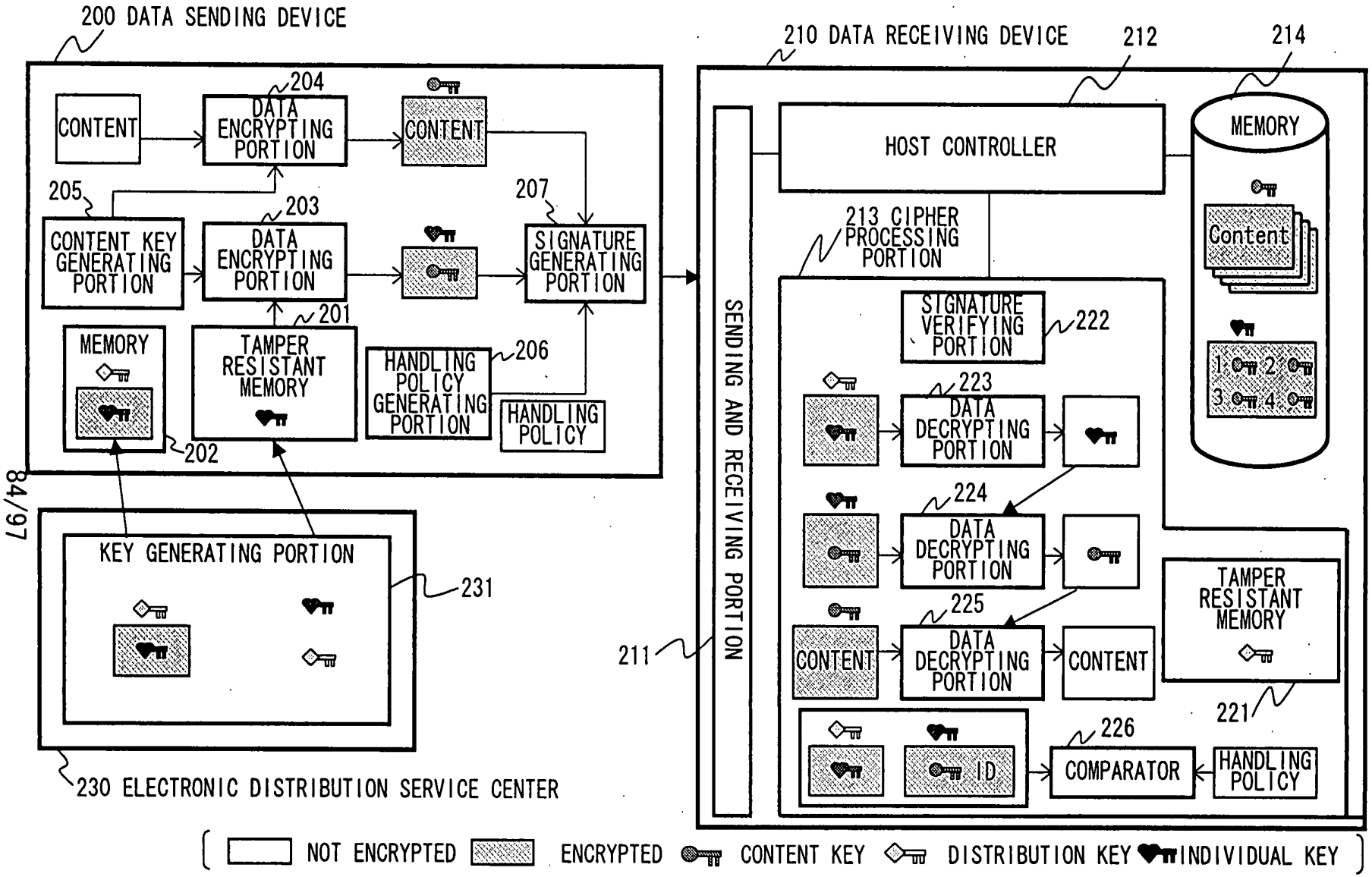
200 DATA SENDING DEVICE
CONTENT
204
DATA ENCRYPTING PORTION
CONTENT
205
CONTENT KEY GENERATING PORTION
203
DATA ENCRYPTING PORTION
207
SIGNATURE GENERATING PORTION
201
MEMORY
TAMPER RESISTANT MEMORY
HANDLING POLICY GENERATING PORTION
206
HANDLING POLICY
202
KEY GENERATING PORTION
231
230 ELECTRONIC DISTRIBUTION SERVICE CENTER
210 DATA RECEIVING DEVICE
212
214
HOST CONTROLLER
MEMORY
Content
1 2 3 4
213 CIPHER PROCESSING PORTION
SIGNATURE VERIFYING PORTION
222
223
DATA DECRYPTING PORTION
224
DATA DECRYPTING PORTION
225
DATA DECRYPTING PORTION
CONTENT
CONTENT
TAMPER RESISTANT MEMORY
221
ID
226
COMPARATOR
HANDLING POLICY
211
SENDING AND RECEIVING PORTION
NOT ENCRYPTED
ENCRYPTED
CONTENT KEY
DISTRIBUTION KEY
INDIVIDUAL KEY

FIG. 84

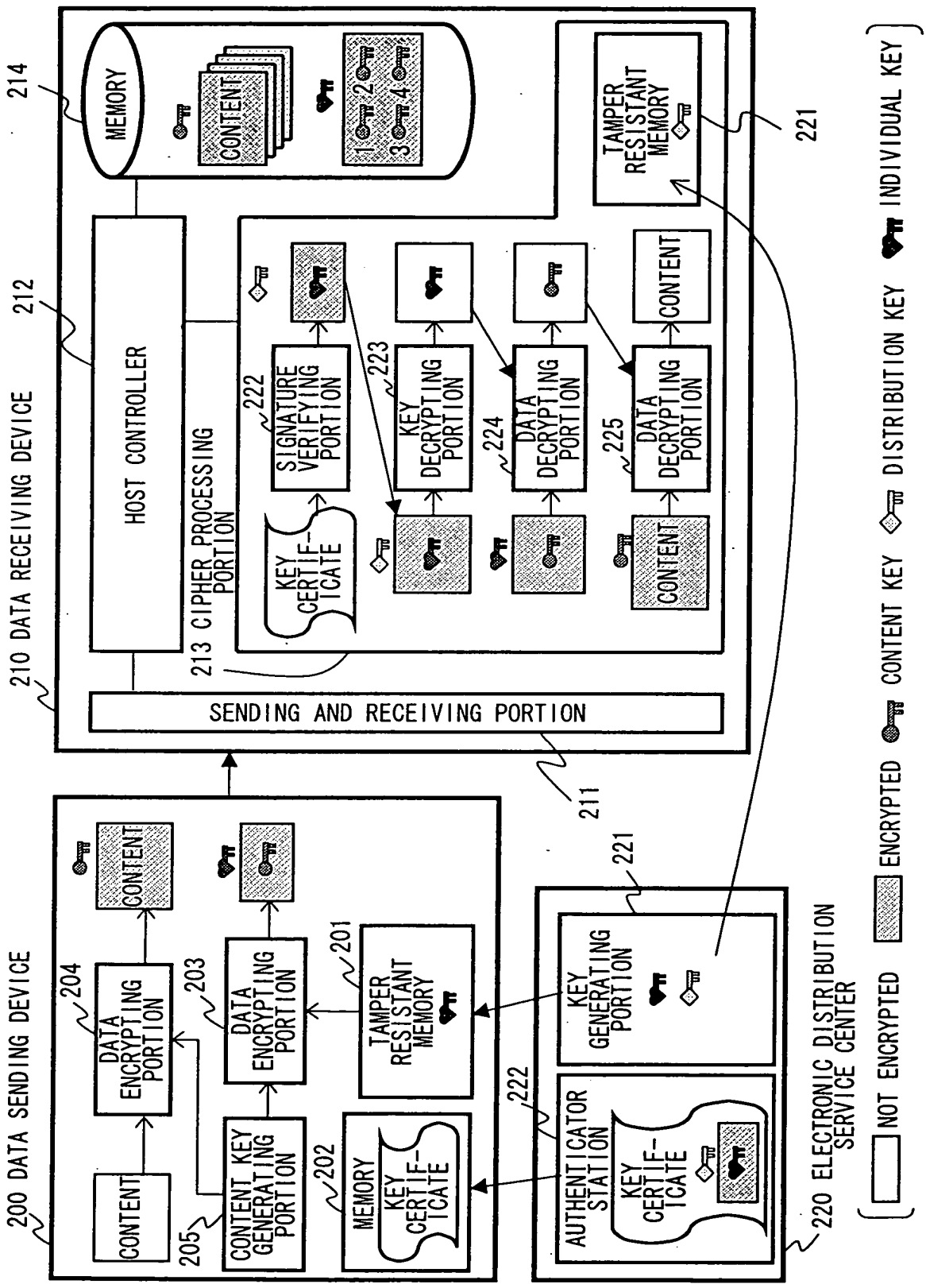
200 DATA SENDING DEVICE
CONTENT
CONTENT KEY GENERATING PORTION
205
202
MEMORY
KEY CERTIF-ICATE
DATA ENCRYPTING PORTION
203
DATA ENCRYPTING PORTION
204
201
TAMPER RESISTANT MEMORY
CONTENT
211
210 DATA RECEIVING DEVICE
212
HOST CONTROLLER
213 CIPHER PROCESSING PORTION
SENDING AND RECEIVING PORTION
214
MEMORY
CONTENT
1 2 3 4
222
SIGNATURE VERIFYING PORTION
KEY CERTIF-ICATE
223
KEY DECRYPTING PORTION
224
DATA DECRYPTING PORTION
225
DATA DECRYPTING PORTION
CONTENT
CONTENT
TAMPER RESISTANT MEMORY
221
220 ELECTRONIC DISTRIBUTION SERVICE CENTER
AUTHENTICATOR STATION
KEY CERTIF-ICATE
222
KEY GENERATING PORTION
221
NOT ENCRYPTED
ENCRYPTED
CONTENT KEY
DISTRIBUTION KEY
INDIVIDUAL KEY

FIG. 85

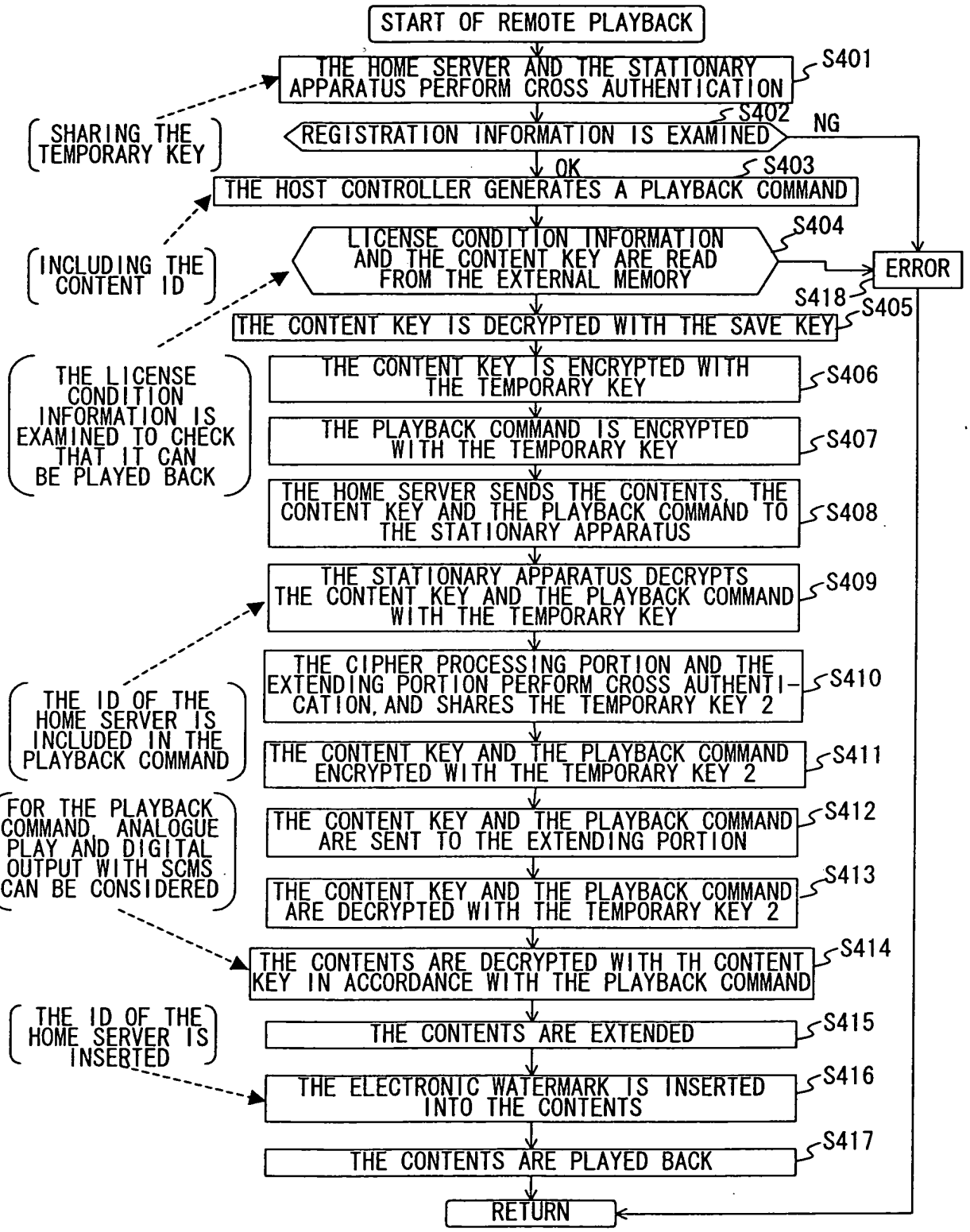
START OF REMOTE PLAYBACK
THE HOME SERVER AND THE STATIONARY APPARATUS PERFORM CROSS AUTHENTICATION
S401
SHARING THE TEMPORARY KEY
REGISTRATION INFORMATION IS EXAMINED
S402
NG
OK
S403
THE HOST CONTROLLER GENERATES A PLAYBACK COMMAND
INCLUDING THE CONTENT ID
LICENSE CONDITION INFORMATION AND THE CONTENT KEY ARE READ FROM THE EXTERNAL MEMORY
S404
ERROR
S418
S405
THE CONTENT KEY IS DECRYPTED WITH THE SAVE KEY
THE LICENSE CONDITION INFORMATION IS EXAMINED TO CHECK THAT IT CAN BE PLAYED BACK
THE CONTENT KEY IS ENCRYPTED WITH THE TEMPORARY KEY
S406
THE PLAYBACK COMMAND IS ENCRYPTED WITH THE TEMPORARY KEY
S407
THE HOME SERVER SENDS THE CONTENTS, THE CONTENT KEY AND THE PLAYBACK COMMAND TO THE STATIONARY APPARATUS
S408
THE STATIONARY APPARATUS DECRYPTS THE CONTENT KEY AND THE PLAYBACK COMMAND WITH THE TEMPORARY KEY
S409
THE ID OF THE HOME SERVER IS INCLUDED IN THE PLAYBACK COMMAND
THE CIPHER PROCESSING PORTION AND THE EXTENDING PORTION PERFORM CROSS AUTHENTICATION, AND SHARES THE TEMPORARY KEY 2
S410
THE CONTENT KEY AND THE PLAYBACK COMMAND ENCRYPTED WITH THE TEMPORARY KEY 2
S411
FOR THE PLAYBACK COMMAND, ANALOGUE PLAY AND DIGITAL OUTPUT WITH SCMS CAN BE CONSIDERED
THE CONTENT KEY AND THE PLAYBACK COMMAND ARE SENT TO THE EXTENDING PORTION
S412
THE CONTENT KEY AND THE PLAYBACK COMMAND ARE DECRYPTED WITH THE TEMPORARY KEY 2
S413
THE CONTENTS ARE DECRYPTED WITH TH CONTENT KEY IN ACCORDANCE WITH THE PLAYBACK COMMAND
S414
THE ID OF THE HOME SERVER IS INSERTED
THE CONTENTS ARE EXTENDED
S415
THE ELECTRONIC WATERMARK IS INSERTED INTO THE CONTENTS
S416
THE CONTENTS ARE PLAYED BACK
S417
RETURN

FIG. 86

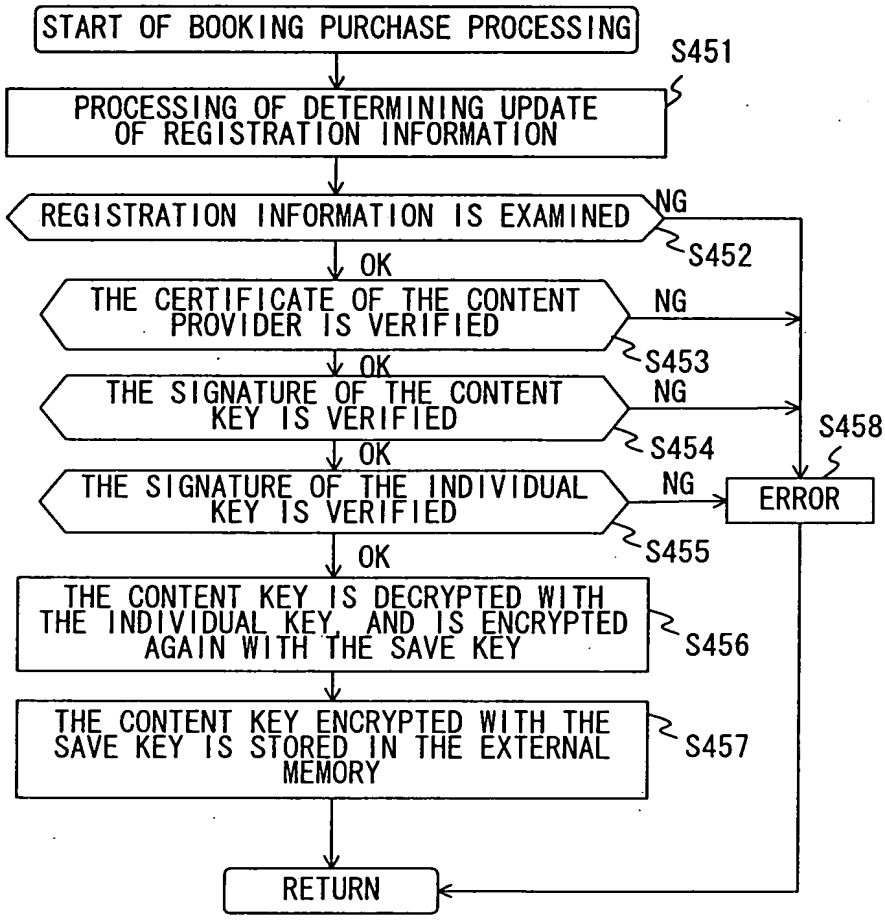
START OF BOOKING PURCHASE PROCESSING
S451
PROCESSING OF DETERMINING UPDATE OF REGISTRATION INFORMATION
REGISTRATION INFORMATION IS EXAMINED
NG
S452
OK
THE CERTIFICATE OF THE CONTENT PROVIDER IS VERIFIED
NG
S453
OK
THE SIGNATURE OF THE CONTENT KEY IS VERIFIED
NG
S454
OK
THE SIGNATURE OF THE INDIVIDUAL KEY IS VERIFIED
NG
S455
OK
S458
ERROR
THE CONTENT KEY IS DECRYPTED WITH THE INDIVIDUAL KEY, AND IS ENCRYPTED AGAIN WITH THE SAVE KEY
S456
THE CONTENT KEY ENCRYPTED WITH THE SAVE KEY IS STORED IN THE EXTERNAL MEMORY
S457
RETURN

FIG. 87

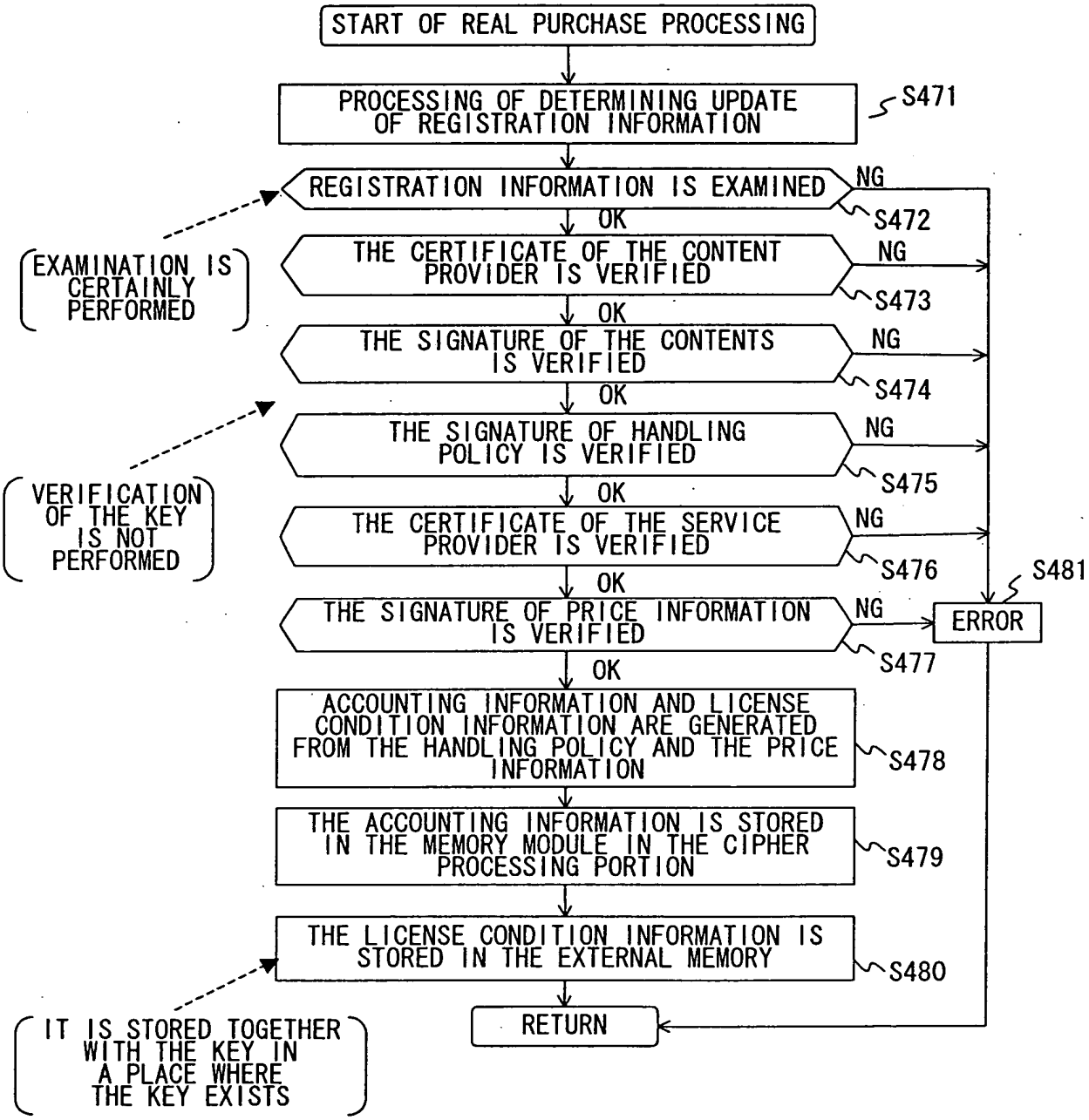
START OF REAL PURCHASE PROCESSING
PROCESSING OF DETERMINING UPDATE OF REGISTRATION INFORMATION
S471
REGISTRATION INFORMATION IS EXAMINED
NG
S472
OK
EXAMINATION IS CERTAINLY PERFORMED
THE CERTIFICATE OF THE CONTENT PROVIDER IS VERIFIED
NG
S473
OK
THE SIGNATURE OF THE CONTENTS IS VERIFIED
NG
S474
OK
THE SIGNATURE OF HANDLING POLICY IS VERIFIED
NG
S475
OK
VERIFICATION OF THE KEY IS NOT PERFORMED
THE CERTIFICATE OF THE SERVICE PROVIDER IS VERIFIED
NG
S476
OK
S481
THE SIGNATURE OF PRICE INFORMATION IS VERIFIED
NG
ERROR
S477
OK
ACCOUNTING INFORMATION AND LICENSE CONDITION INFORMATION ARE GENERATED FROM THE HANDLING POLICY AND THE PRICE INFORMATION
S478
THE ACCOUNTING INFORMATION IS STORED IN THE MEMORY MODULE IN THE CIPHER PROCESSING PORTION
S479
THE LICENSE CONDITION INFORMATION IS STORED IN THE EXTERNAL MEMORY
S480
IT IS STORED TOGETHER WITH THE KEY IN A PLACE WHERE THE KEY EXISTS
RETURN

FIG. 88

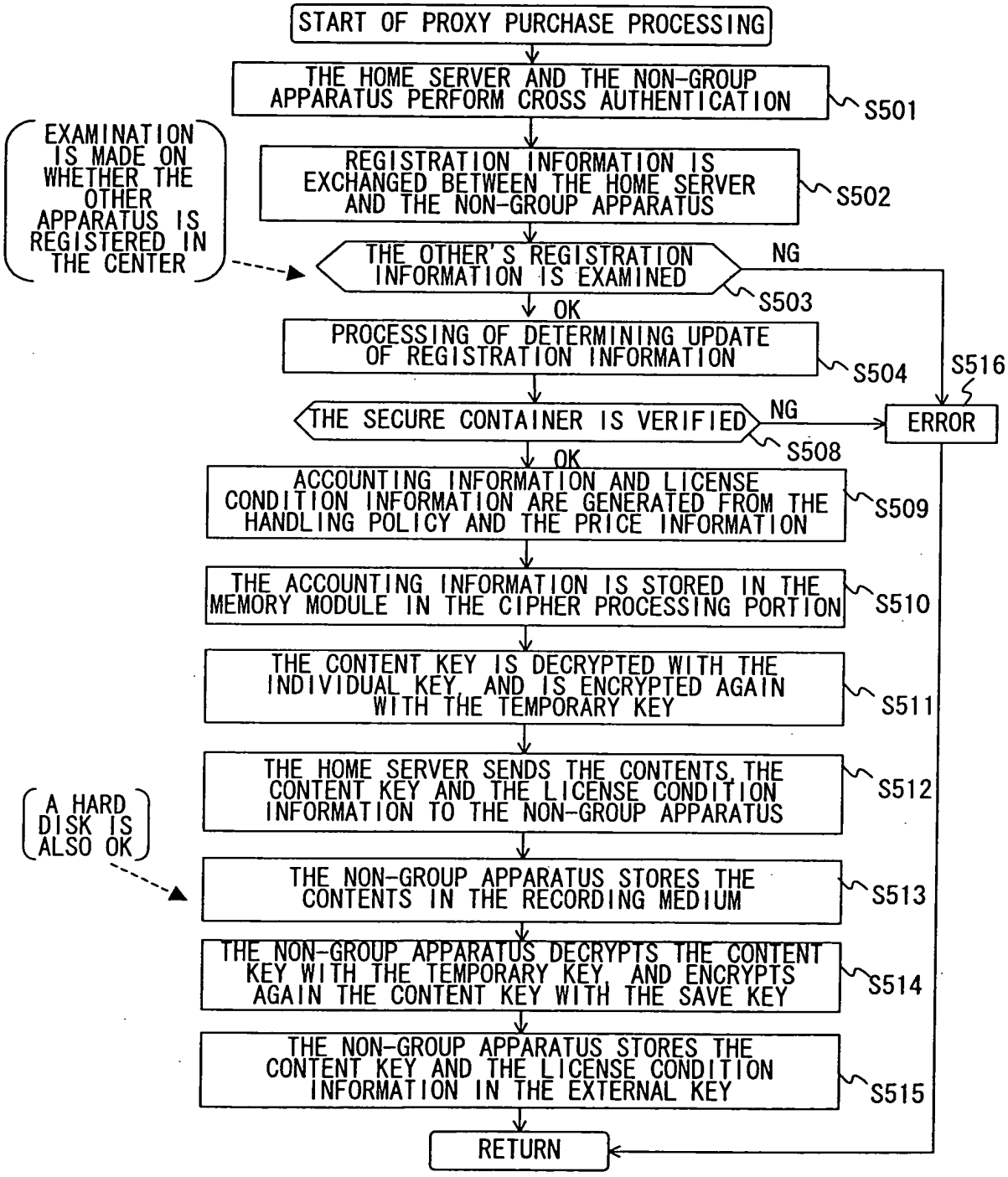
START OF PROXY PURCHASE PROCESSING
THE HOME SERVER AND THE NON-GROUP APPARATUS PERFORM CROSS AUTHENTICATION
S501
EXAMINATION IS MADE ON WHETHER THE OTHER APPARATUS IS REGISTERED IN THE CENTER
REGISTRATION INFORMATION IS EXCHANGED BETWEEN THE HOME SERVER AND THE NON-GROUP APPARATUS
S502
THE OTHER'S REGISTRATION INFORMATION IS EXAMINED
NG
S503
OK
PROCESSING OF DETERMINING UPDATE OF REGISTRATION INFORMATION
S504
S516
THE SECURE CONTAINER IS VERIFIED
NG
ERROR
S508
OK
ACCOUNTING INFORMATION AND LICENSE CONDITION INFORMATION ARE GENERATED FROM THE HANDLING POLICY AND THE PRICE INFORMATION
S509
THE ACCOUNTING INFORMATION IS STORED IN THE MEMORY MODULE IN THE CIPHER PROCESSING PORTION
S510
THE CONTENT KEY IS DECRYPTED WITH THE INDIVIDUAL KEY, AND IS ENCRYPTED AGAIN WITH THE TEMPORARY KEY
S511
THE HOME SERVER SENDS THE CONTENTS, THE CONTENT KEY AND THE LICENSE CONDITION INFORMATION TO THE NON-GROUP APPARATUS
S512
A HARD DISK IS ALSO OK
THE NON-GROUP APPARATUS STORES THE CONTENTS IN THE RECORDING MEDIUM
S513
THE NON-GROUP APPARATUS DECRYPTS THE CONTENT KEY WITH THE TEMPORARY KEY, AND ENCRYPTS AGAIN THE CONTENT KEY WITH THE SAVE KEY
S514
THE NON-GROUP APPARATUS STORES THE CONTENT KEY AND THE LICENSE CONDITION INFORMATION IN THE EXTERNAL KEY
S515
RETURN

FIG. 89

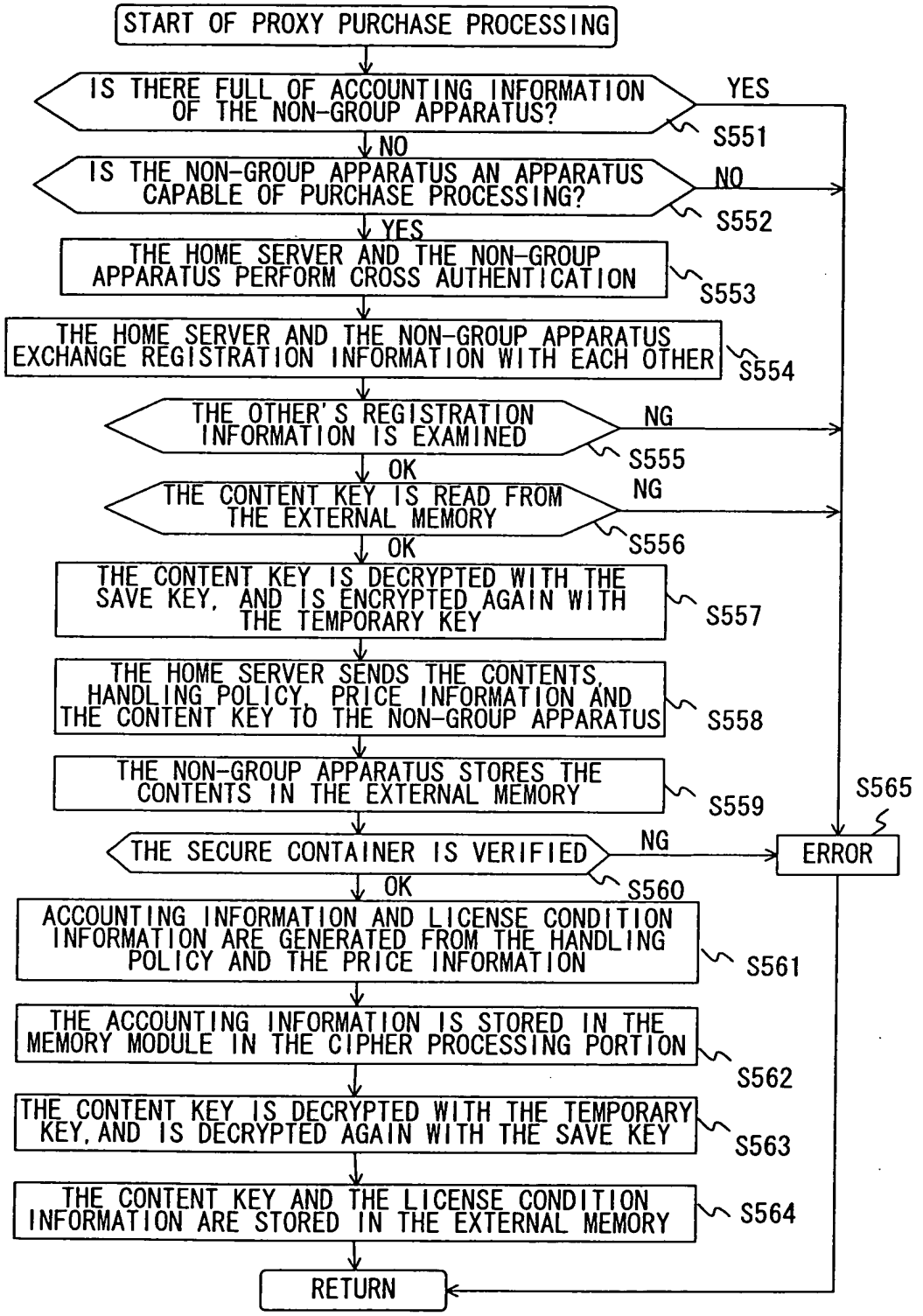

FIG. 90

09830392 - 062100

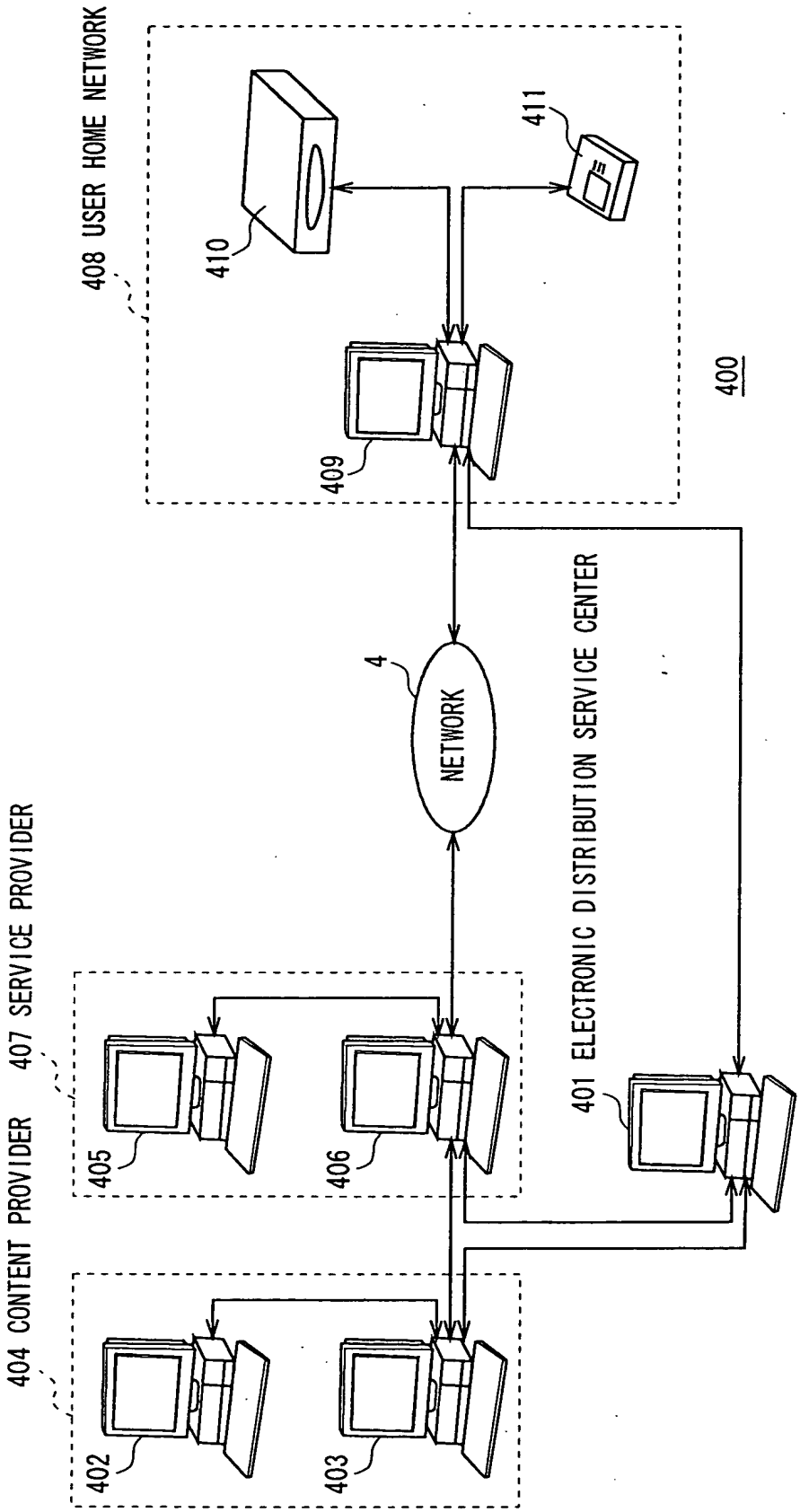
408 USER HOME NETWORK
410
411
409
400
4
NETWORK
401 ELECTRONIC DISTRIBUTION SERVICE CENTER
404 CONTENT PROVIDER
407 SERVICE PROVIDER
405
406
402
403

FIG. 91

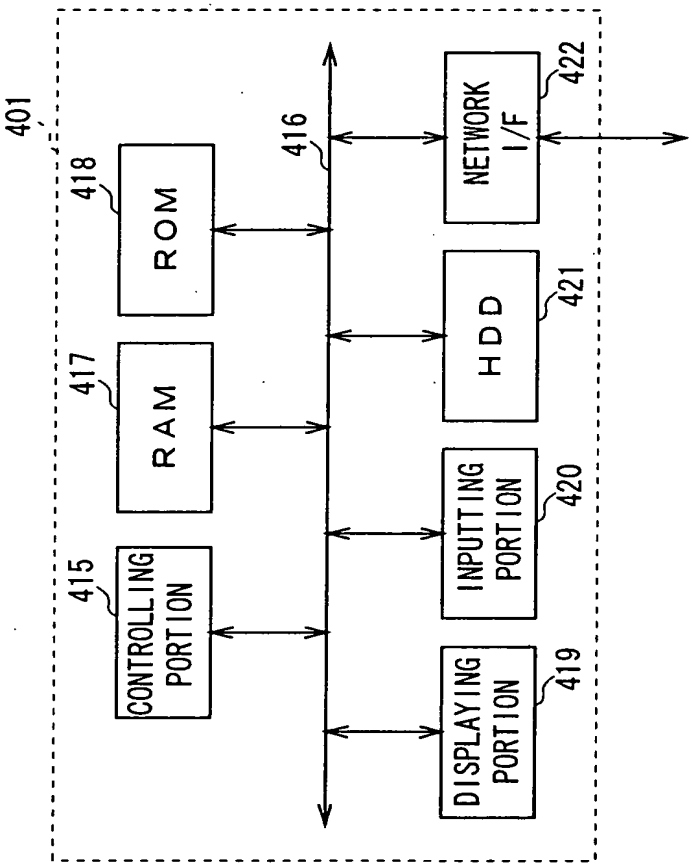
401
418
ROM
417
RAM
415
CONTROLLING PORTION
416
NETWORK I/F
422
HDD
421
INPUTTING PORTION
420
DISPLAYING PORTION
419

FIG. 92

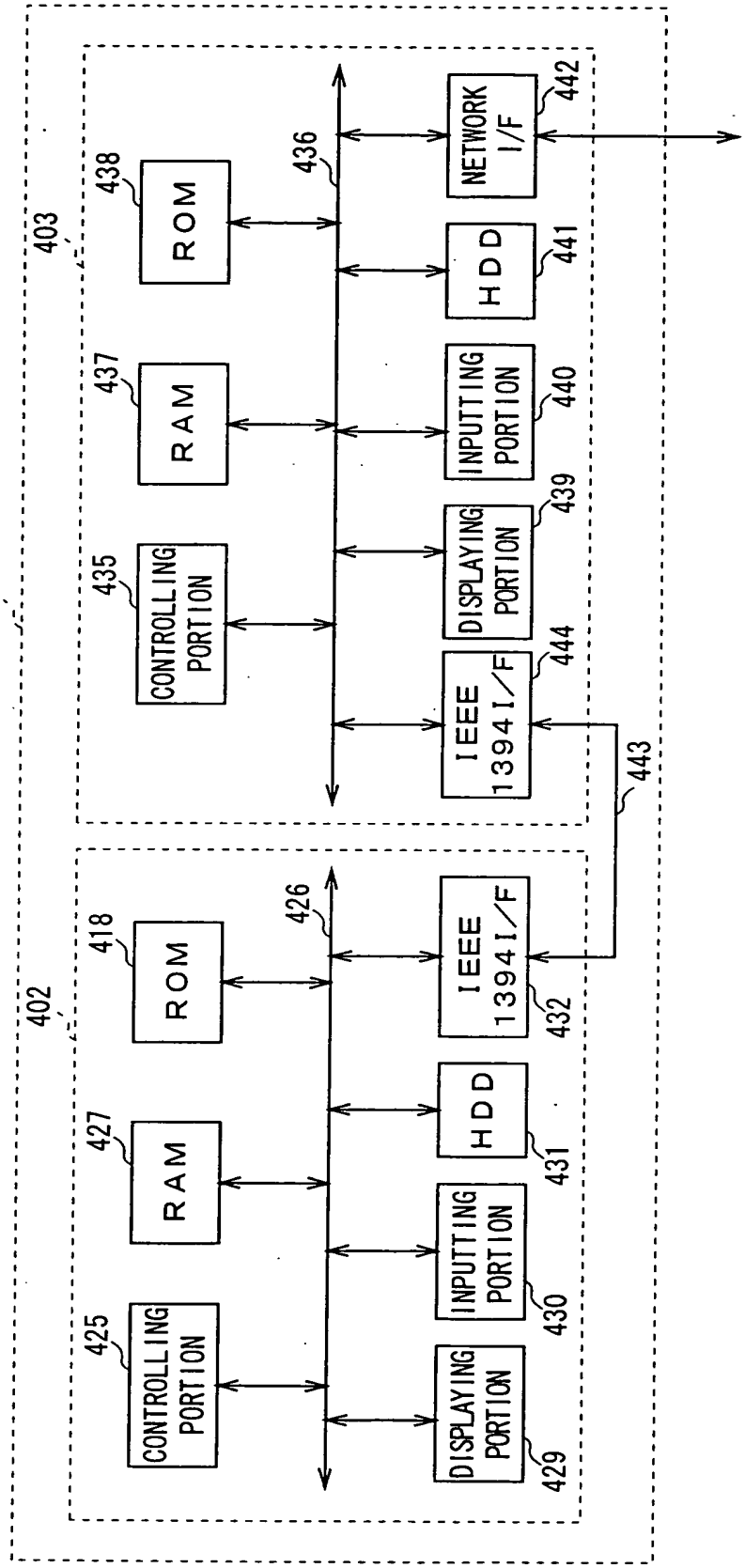
404
403
402
438
ROM
437
RAM
435
CONTROLLING PORTION
436
NETWORK I/F
442
HDD
441
INPUTTING PORTION
440
DISPLAYING PORTION
439
IEEE 1394I/F
444
443
418
ROM
427
RAM
425
CONTROLLING PORTION
426
IEEE 1394I/F
432
HDD
431
INPUTTING PORTION
430
DISPLAYING PORTION
429

FIG. 93

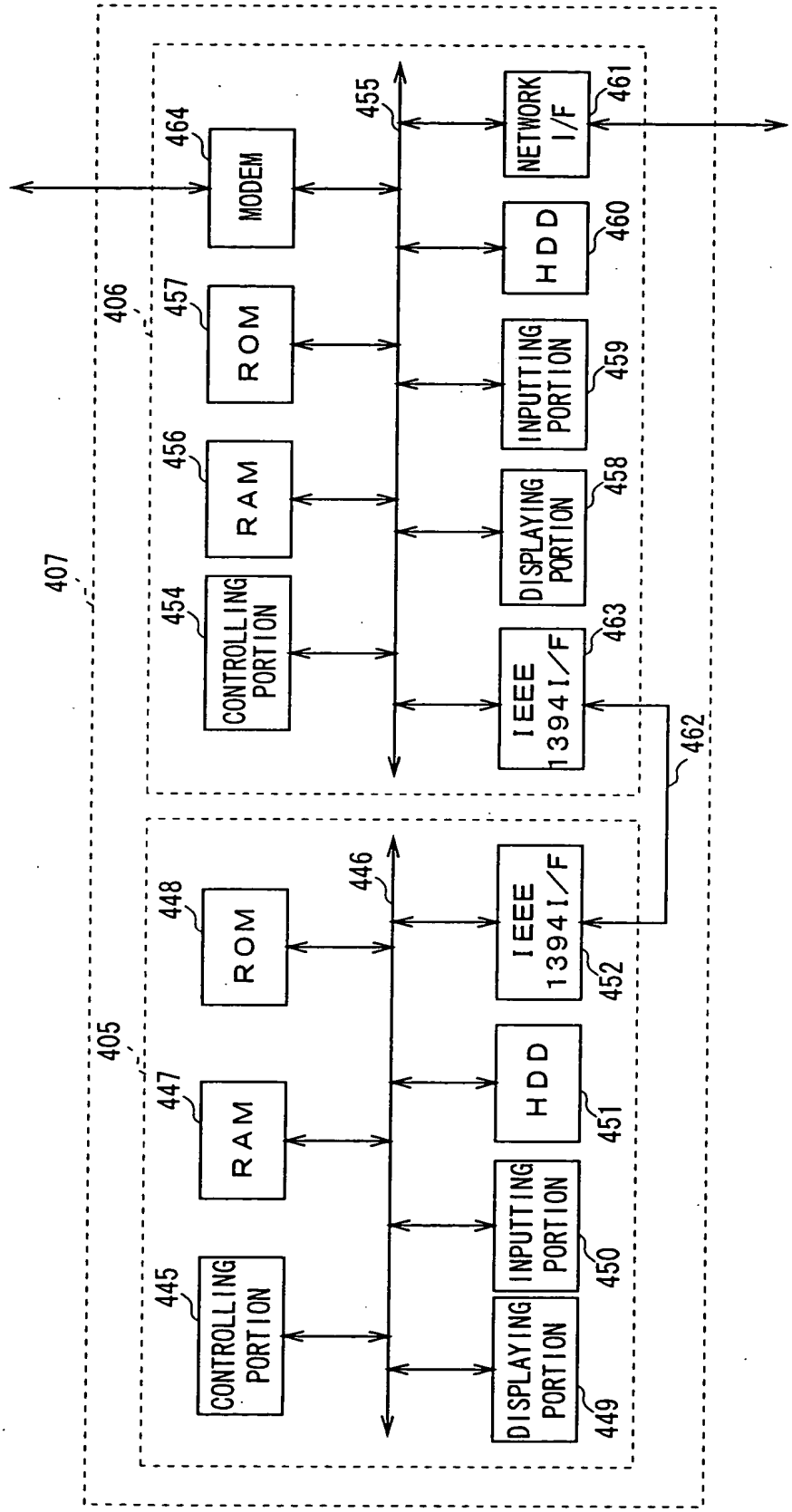
407
406
405
464
MODEM
455
NETWORK I/F
461
457
ROM
HDD
460
456
RAM
INPUTTING PORTION
459
454
CONTROLLING PORTION
DISPLAYING PORTION
458
IEEE 1394I/F
463
462
448
ROM
446
IEEE 1394I/F
452
447
RAM
HDD
451
445
CONTROLLING PORTION
INPUTTING PORTION
450
DISPLAYING PORTION
449

FIG. 94

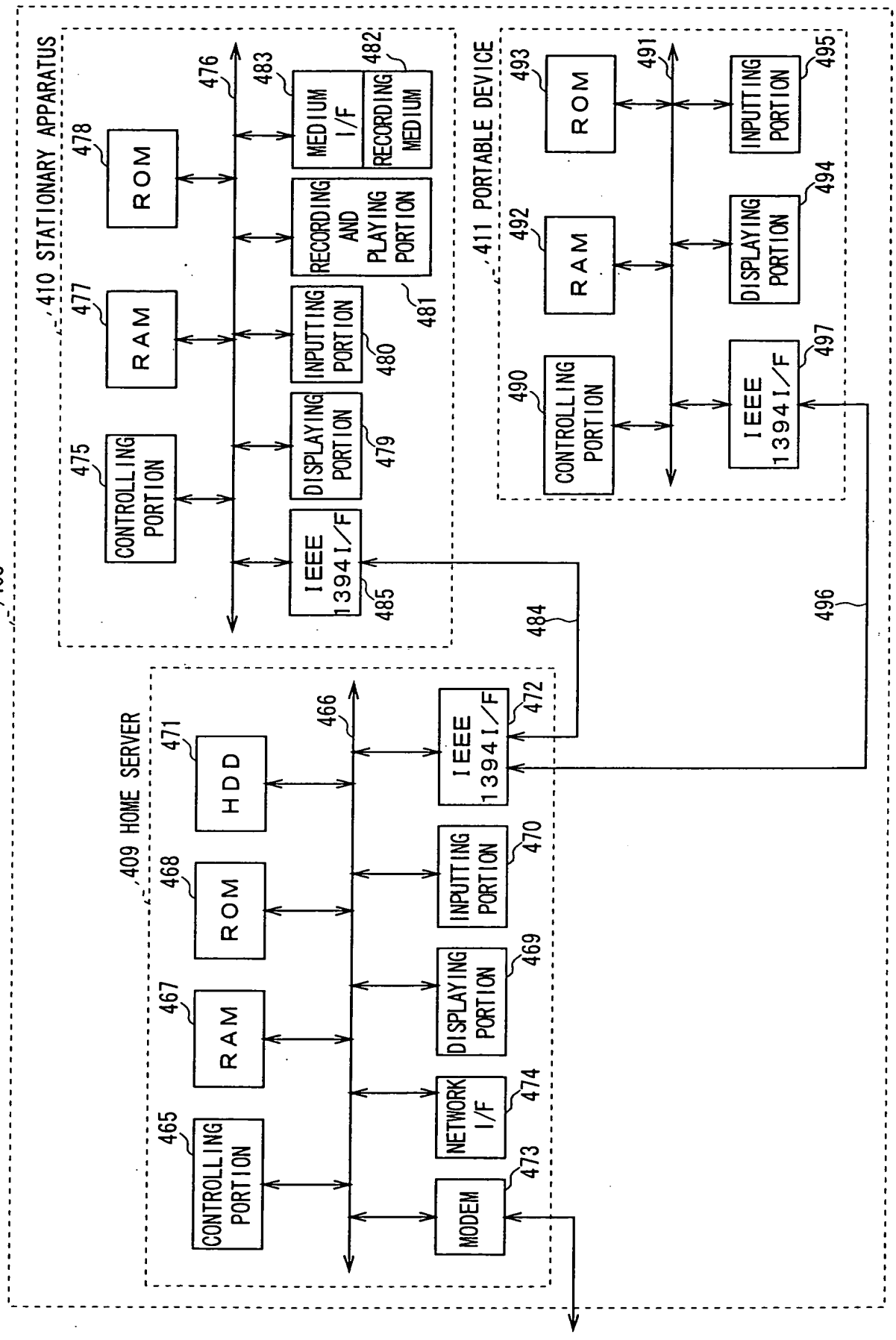
408
409 HOME SERVER
410 STATIONARY APPARATUS
411 PORTABLE DEVICE
CONTROLLING PORTION
RAM
ROM
HDD
MODEM
NETWORK I/F
DISPLAYING PORTION
INPUTTING PORTION
IEEE 1394I/F
RECORDING AND PLAYING PORTION
MEDIUM I/F
RECORDING MEDIUM
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
490
491
492
493
494
495
496
497

FIG. 95

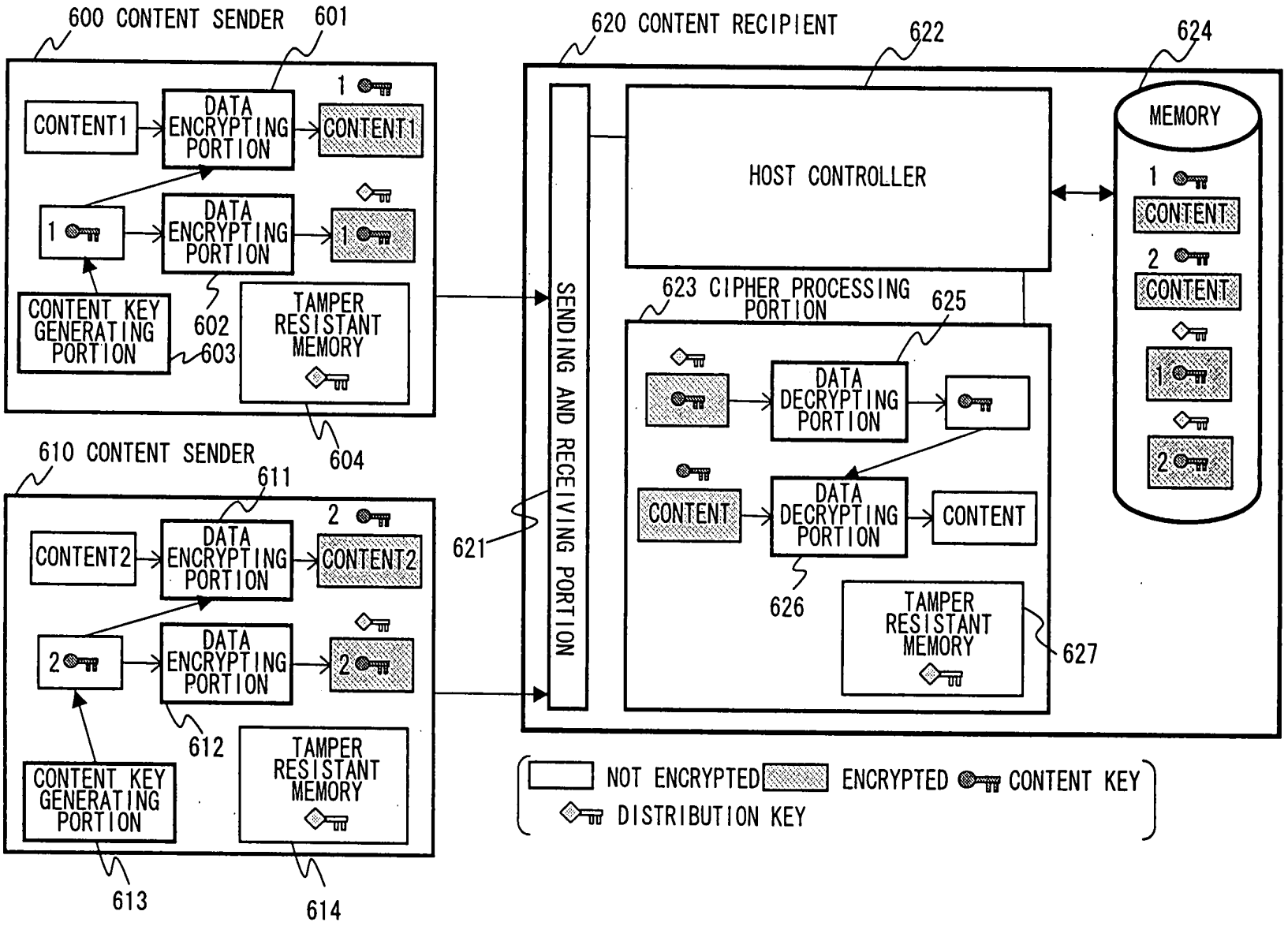

FIG. 96

09/830392

Explanation of Reference Numerals

1, 401...electronic distribution service center, 2, 404...content provider, 3, 407...service provider, 4...network, 5, 408...user home network, 10, 400...electronic music distribution system, 11...service provider managing portion, 12...content provider managing portion, 13...copyright managing portion, 14...key server, 15...background data managing portion, 16...benefit distributing portion, 17...cross authenticating portion, 18...user managing portion, 19...account charging portion, 20...banking portion, 21...auditing portion, 22...authenticator station, 23...content server, 24...content authoring portion, 31...content server, 32...electronic water adding portion, 34...content encrypting portion, 35...content key generating portion, 36...content key encrypting portion, 37...handling policy generating portion, 38...signature generating portion, 39...cross authenticating portion, 41...content server, 42...certificate verifying portion, 43...signature verifying portion, 44...pricing portion, 45...signature generating portion, 46...cross authenticating portion, 51, 409...home server, 52, 410...stationary apparatus, 53, 411...portable device, 62, 72, 82...host controller, 56, 73, 83...cipher processing portion, 66, 74, 84...extending portion, 67, 79, 85...external memory, 120...electronic distribution only recording medium, 402, 405...personal computer for servers, 403, 406...signal processing personal computer